PowerDsine™ The Power over Ethernet Pioneers

PowerDsine Power View Pro

Power over Ethernet
Remote Web Manager

User Guide

Release 1.1

Cat. No. 06-1213-056

Notice

The information contained herein is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, PowerDsine cannot accept responsibility for inadvertent errors, inaccuracies, subsequent changes or omissions of printed material.

PowerDsine Ltd. reserves the right to make changes to products and to their specifications as described in this document, at any time, without prior notice. No rights to any PowerDsine Ltd. Intellectual property are licensed to any third party, either directly, by implication or by any other method.

Acknowledgements

All other products or trademarks are property of their respective owners.

The product described by this manual is a licensed product of PowerDsine.

Abbreviations and Terminology

Abbreviations are spelled out in full when first used. Only industry-standard terms are used throughout this manual.

Note: Covered under U.S patent S/N 6,473,608. Other Patents pending

Table of Contents

List of Figures

List of Tables

1 About this Guide

1.1 Objectives

This User Guide introduces PowerDsine's Power View Pro Remote Web Manager which is used for managing PowerDsine's Power over Ethernet (PoE) product line of Midspan devices including:

- PD- 6524 – 24 ports
- PD -6512 – 12 ports
- PD -6506 – 6 ports

1.2 Audience

This Guide is intended for network administrators, supervisors and installation technicians who have a background in:

- Basic concepts and terminology of networking
- Network toPoEogy
- Protocols
- Microsoft Windows environment

1.3 Organization

This Guide is divided into several Sections, as follows:

Section 1 - Defines the overall concepts used in this Guide, conventions used and associated documentation.

Section 2 - Describes the Power View Pro features and capabilities.

Section 3 – Provides a complete system installation procedure.

Section 4 - Provides the GUI detailed description.

Section 5 - Provides how to use the PowerView Pro GUI.

Section 6 – Provides troubleshooting guide

Section 7 – Provides upgrading Midspan software process.

1.4 Conventions

The various conventions used in defining commands and examples are given in Table 1-1.

Table 1-1: Conventions Used

CONVENTION	DEFINITION
bold	**Keywords & commands**
italics	*Represents a GUI item*
`screen`	`Displayed Information`
`Bold screen`	**`Information to be entered`**
Notes	Helpful information

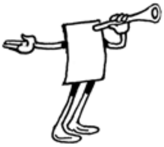
1.5 Related Documentation

For additional information, refer to the following documentation:

- Power over Ethernet PowerDsine PD-60XX (AC and DC version), User Manual (06-6800-056).
- IEEE Standard 802.3af, DTE Power via MDI.

1.6 Abbreviations

PoE	Power over Ethernet
NTP	Network Time Protocol
DES	Data Encryption Standard
MD5	Message Digest 5
MDI	Multiple-Document Interface
MIB	Management Information Base
PD	Powered Device
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
FTP	File Transfer Protocol
TFTP	Trivial File Transfer Protocol



2 Introducing the Power View Pro

2.1 Overview

PowerDsine's Power View Pro is a management system, utilized for complete monitoring and control of PowerDsine's Power over Ethernet (PoE) Midspans, via remote network management station. The system provides direct on-line power supervision, configuration, monitoring and diagnostics of PowerDsine products via their SNMP managers.

2.2 Features

The manager provides a number of unique features for PoE Midspan management as follows:

- Web-based for remote management of Power over Ethernet device
- Secured WEB based configuration (SSL)
- Configuration using graphical representations of remote device
- Real time monitoring with visual status
- System status display
- Real time power parameters
- SNMPv2c/v1/v3
- Power over Ethernet (PoE) SNMP MIBs
- Log events to remote SysLog Server

2.3 System Capabilities

The manager can be accessed from any computer by WEB browser such as an Internt Explorer/Netscape, SNMP management station, Telnet, or RS232 Terminal. The Power View Pro allows monitoring and controlling of over Etehrnet IP networks as shown in Figure 2-1:

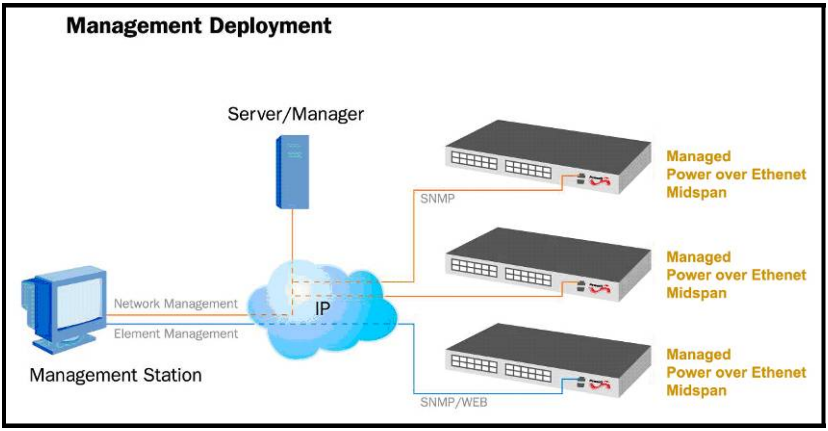


Figure 2-1: Management Deployment

2.3.1 Configuration options

- Web based – by utilizing a WEB browser
- SNMP – by utilizing an SNMP management application on a remote computer
- Telnet – via the RJ45 Etehrnet port by using Telent application on a remote computer
- Serial communication port – by using Terminal emulation software such as Microsoft Windows Hyper Terminal, or any similar software.
- Serial communication rate must be set to 38400, no hardware flow control and cross cable should be used (pin2 crossed with pin3).

NOTE:

The unit is shipped with default IP of 192.168.0.50. Make sure that a computer Network card is configured to the same IP network.

- Telnet and WEB configuration are password protected.
- Serial communication configuration should be used only in order to define unit's IP address, or in order to perform software updates. Any other configuration should be carried out via the WEB browser.

2.4 Security & User Authentication

2.4.1 Web Configuration

Web configuration can be protected by user by password. Two user & password protection levels are avilable as follows:

- **View username & password –** a remote user has access to Web pages that provide various information, but has no permition to perform any modifications.

- **Configuration username & password -** a remote user (usually administrator) has full authority to modify any unit's parameter.

2.4.2 SNMP

- **SNMP v1/v2** - community string is utilized for authentication Get/Set/Trap authentication.

- **SNMP v3 –** Network Management Protocol Version-3 (SNMPv3) is an standards-based protocol, utilized for network management. It provides secure access to devices by a combination of authenticating and encrypting packets over the network.

2.4.3 Telnet Configuration

Since Telnet provide access to software updates and data bases for upload/download functions, it is always password protected (regrdless of Web view & configure passoword selection option).

WEB and Telnet utilize the same passwords (Telnet utilizes Web browser password even if the Web password function is disabled).

NOTE:

The Power View Pro is provided with the following factory defaults:

Protection:

Configuration password protection

WEB/Telnet:

View *(usually user) : user name ="**user**", password ="**password**"*

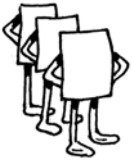
Configure *(usually administrator)**:** user name ="**admin**", password = "**password**".*

SNMP v3:

Guest *(usually remote SNMP manager) : user name ="**public"***

View User *(usually user) **:** user name ="**view**", authentication password (MD5) = "**password**", **:** privacy password (DES)= "**password**",*

Admin User *(usually administrator) **:** user name ="**admin**", authentication password (MD5) = "**password**", **:** privacy password (DES)= "**password**",*



3 Installation

3.1 Installation

3.1.1 Configuration Options

The following configuration options are available:

- Via an RJ-45 network connector utilizing a Web browser (IP 192.168.0.50)
- Via an RJ-45 network connector utilizing the Telnet protocol.
- Via an RS-232 Serial communication port, utilizing an RS-232 connector (38400, HW flow control off)

NOTE:

This section describes the configuration procedure via the CLI commands. Configuration of system parameters Via the Web browser is further detailed in Paragraph 5.6 on page 60.

3.2 System Requirements

The following hardware/software items are required in order to configure and operate the Power over Ethernet (PoE) Midspan.

- ♦ **Computer Environment**
  - Ethernet Network card
  - Operating system: Any Host with WEB browser
  - Recommended OS & Web browsers:
    - √ Win2000/XP running Microsoft Internet explorer Ver6 or higher
    - √ Win2000/XP running Netscape 7 or higher
    - √ Access to a local network and Internet
    - √ PC network card configured to the following parameters:

      IP NET: 192.168.0.50, **IP Mask**:255.255.255.0
  - Ethernet cable.
  - Telnet application
  - Serial Communication
    - √ Serial ports: COM1 or COM2 are active and available
  - Null-modem RS232 crossed cable
- ♦ **Administrative Requirements**
  - Free IP address to be allocated for the PoE Midspan (192.168.0.50 is provided by PowerDsine as a default address), or obtained by using the DHCP server.

3.3 Hardware Setup

Perform the following steps (see Figure 3-1):

Connect an AC power cable to the PoE unit and verify that all LEDs illuminate once (self test).

Connect the crossed null-modem cable between the management station COM port and the PoE RS-232 port (optional)

Connect a network cable between the PoE unit front panel's RJ45 connector and the Ethernet.

1 Verify that the *AC* LED on the front panel is lit and that the *Link* LED is green.

If any problem is encountered during setup, refer to Chapter. 6, Troubleshooting":

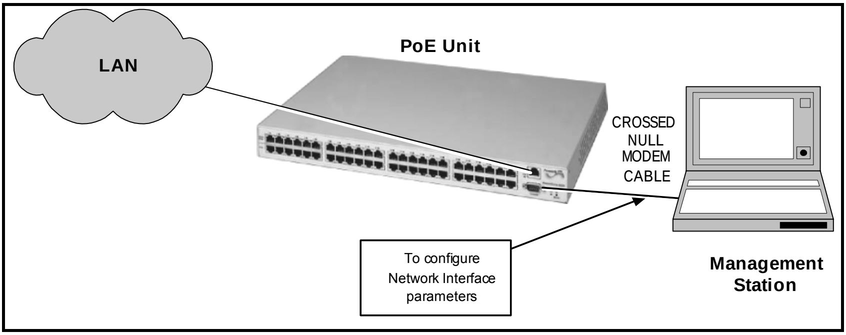


Figure 3-1: Connecting the PoE Unit

3.4 Installation Procedure

3.4.1 Web Browsing

Open Web browser and type *192.168.0.50* in the address field.

3.4.2 Telnet Browsing

- Go to **start -> Run**
- Type the command **cmd**
- In the window type the command, **telnet [IP ADDRESS]**
- Type the Username & password

NOTE:

Use Web browser to view System Configuration->Security WEB page and make sure that the Telnet checkbox is checked (selected) - see page 48.

3.4.3 RS232 Configuration using Hyper Terminal Application

For WIN 2000 and WIN XP users:

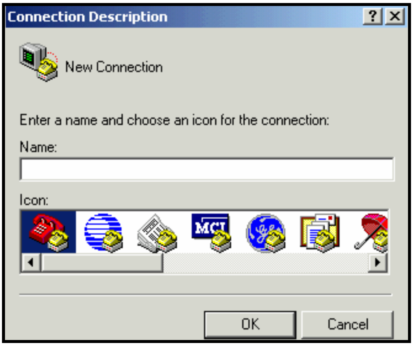
2 Go to ***Run*** (***Start***> ***Run***).

3 Type "***cmd***". A DOS type window opens;
click **OK**.

4 Type the "***ipconfig"*** and then click ***Enter***.

1 Note computer IP, mask and default gateway.

2 Click *Start* > *Programs* > *Accessories* > *Communications* > *HyperTerminal*, A dialog box appears.



Connection Description

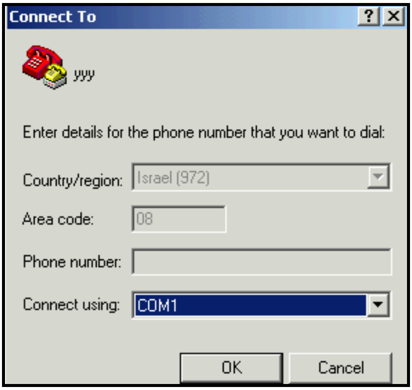
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

3 Enter your name or organization name in the *Name* text field and then click *OK*; *Connect To* window appears.



Connect To

yyy

Enter details for the phone number that you want to dial:

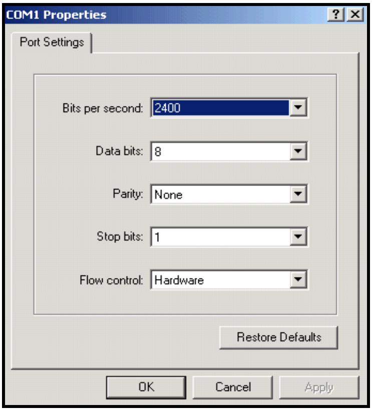
Country/region: Israel (972)

Area code: 08

Phone number:

Connect using: COM1

4 Select the desired communication port to be connected to the PoE unit and then click *OK*. A dialog window appears;



COM1 Properties

Port Settings

Bits per second: 2400

Data bits: 8

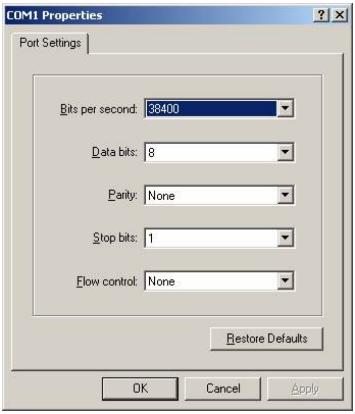
Parity: None

Stop bits: 1

Flow control: Hardware

5 Select the following parameters and then click *OK*:

```
Bits per second: 38400
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None
```



COM1 Properties

Port Settings

Bits per second: 38400

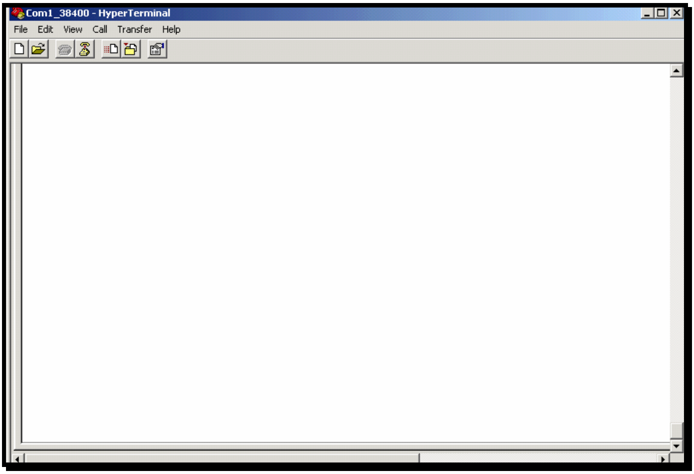
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

5 The HyperTerminal screen appears;



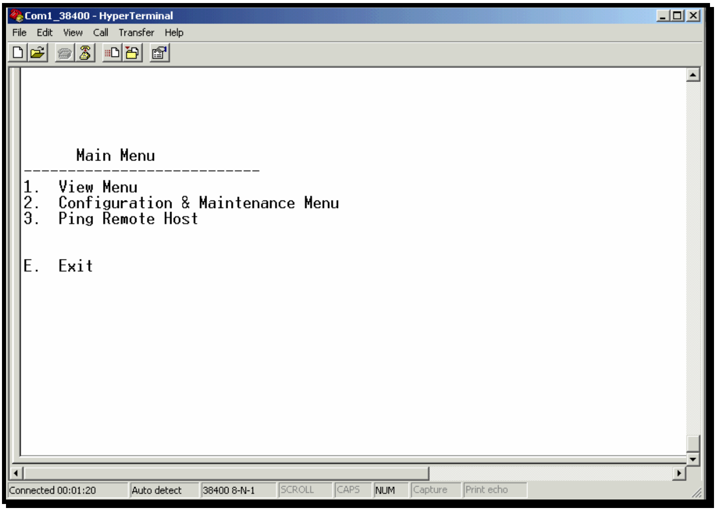
3.4.4 Configuring the System via the HyperTerminal

NOTE:

There is no password protection while using the RS232 serial communication port. Password protection is only applicable for Telnet or WEB access.

Perform the following steps:

1 Click the ESC or space key: the main menu appears:



```
      Main Menu
---------------------------
1.  View Menu
2.  Configuration & Maintenance Menu
3.  Ping Remote Host


E.  Exit
```

Main Menu

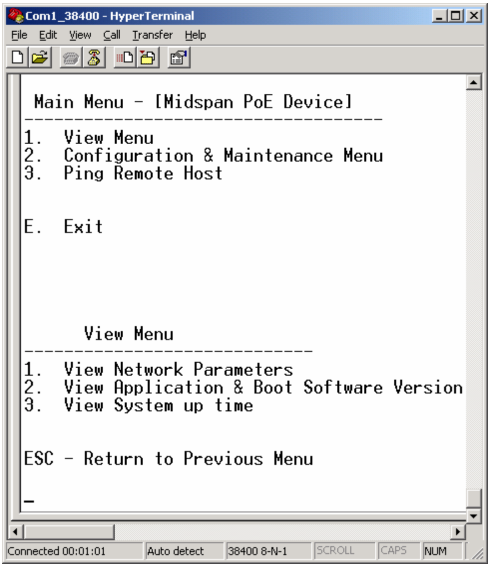
----

1. ***View Menu*** – view unit IP, software version and release date.
2. ***Configuration* & Maintenance Menu** - Configure unit IP, upload/download configuration & software update
3. ***Ping Remote Host*** – determine whether a particular IP system on a network is functional. Used for diagnosing IP network or router failures.

E. ***Exit*** – exits terminal main menu

3.4.5 Using the View Menu

1 Select the *View Menu* option; *View Menu* appears;



```
 Main Menu - [Midspan PoE Device]
------------------------------------
1.   View Menu
2.   Configuration & Maintenance Menu
3.   Ping Remote Host


E.   Exit





      View Menu
-----------------------------
1.   View Network Parameters
2.   View Application & Boot Software Version
3.   View System up time


ESC - Return to Previous Menu

_
```

View Menu

----

1. ***View Network Parameters* –** such as IP Address, Subnet Mask, Default Gateway and MAC Address.

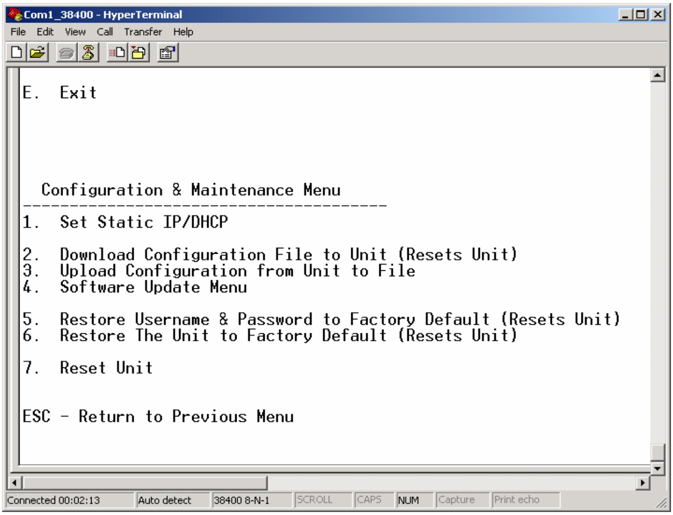
NOTE:

While DHCP is in use, DHCP server IP appears as well.

2. ***View Application & Boot Software Version* –** allows viewing of application version number and creation date.
3. **View system up time –** displays how many days, hours, minutes & seconds the unit has been operational.

3.4.6 Using the Configuration & Maintenance Menu

1 Select the *Configuration & Maintenance Menu* from the *Main Menu*; the following menu appears;



```
E.   Exit



  Configuration & Maintenance Menu
---------------------------------------
1.   Set Static IP/DHCP

2.   Download Configuration File to Unit (Resets Unit)
3.   Upload Configuration from Unit to File
4.   Software Update Menu

5.   Restore Username & Password to Factory Default (Resets Unit)
6.   Restore The Unit to Factory Default (Resets Unit)

7.   Reset Unit


ESC - Return to Previous Menu
```

Configuration & Maintenance Menu

----

1. ***Set Static IP/DHCP –*** allows the user to set, save & activate new network parameters.
2. ***Download Configuration File to Unit (Resets Unit) –*** downloading configuration file from a remote Host named nms.db, using TFTP application (Host must run TFTP server application prior to using this option - see Para. 3.5).

NOTE:

Upon successful downloading, the unit resets itself.

3. **Upload Configuration from Unit to File** – the unit uploads its Internal configuration file named nms_out.db to the Host, utilizing TFTP application (Host must run TFTP server application prior to using this option - see Para. 3.5).

NOTE:

Upon successful downloading, the unit resets itself.

4. ***Software Update Menu*** **-** allows the user to update unit software/firmware

NOTE:

Host must run TFTP server application and appropriate software update package should be available to the user.

5. ***Restore Username&Password to Factory Default –*** restores only view/configure user name & passoword to default values (resets the unit).
6. ***Restore the Unit to Factory Default -*** restores entire unit configuration to factory default values (resets the unit).
7. ***Reset Unit –*** performs reset of the unit.

ESC - Return to Previous Menu

3.4.7 Using the Ping Remote Host Menu

The *Ping Remote Host* Menu is utilized to test the TCP/IP configuration by using the ping command; the user enters the remote IP address

The ping command uses the ICMP echo request and echo reply packets to determine whether a particular IP system on a network is functional. Ping is useful for diagnosing IP network or router failures.

3.5 TFTP Server Configuration

The TFTP Server allows tranfer of files stored by the Host to/from the PoE unit. This paragraph describes how to configure the TFTP server which is utilized for optional software updates.

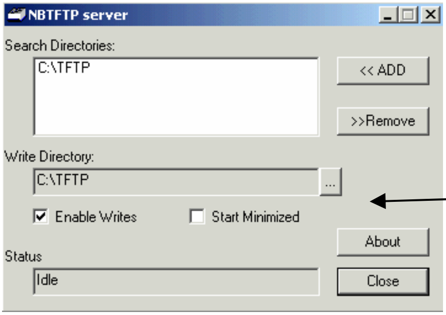
NOTES:

1. Verify that the computer used as a server is always on.
2. Verify that the TFTP server software is running.
3. *Enable Writes* checkbox is checked when *Upload Configuration from Unit to File* is activated by the HyperTerminal menu (see Para. 3.4.6)

1 Set-up a computer to act as a TFTP server.

2 Copy the NBTFTP.exe command from the provided CD to your server□s desktop.

3 Click on the NBTFTP.exe. The following window appears;



NBTFTP server

Search Directories: C:\TFTP

Write Directory: C:\TFTP

☑ Enable Writes

□ Start Minimized

Status: Idle

Browse button

6

7 Click the ***Browse*** button and select your preferred location for the files. Click ***OK*** when done.

4 The Server utilizes the IP address of the computer on which TFTP software is running.

4 GUI Description

4.1 Overview

The GUI (Graphic User Interface) provides complete monitoring, control and configuration of PowerDsine's Power over Line (PoE) products. The GUI is user friendly and presents graphical elements of the actual device in addition to information tables. The system provides several features:

- ♦ Graphical view of the monitored device
- ♦ SNMP Alarms (Traps) notification table for the device being monitored
- ♦ Properties of the management system.

The GUI provides two authorization levels as follows (see also Paragraph 4.4.4.1):

- **System User -** allowed to use the View menu only
- **System administrator** allowed to view and modify all the GUI functions

4.2 Opening Screen

The Main screen (*Opening* screen) window is shown in Figure 4-1. The *Opening* screen features three main menus as follows:

- ♦ View menu – used to view status, network configuration and product information
- ♦ System Configuration menu – allows system Configuration (network, SNMP, security, product parameters and maintenance (it is password protected)
- ♦ Port Configuration menu – allows enabling/disabling of ports, allocation of power, setting of priorities and more.

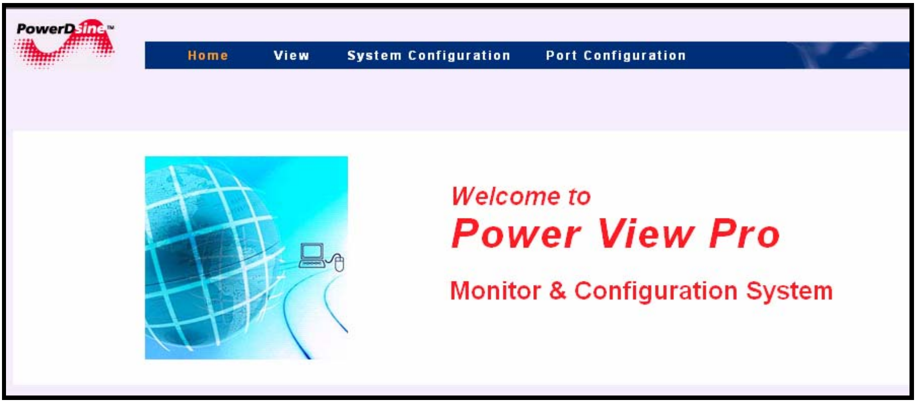
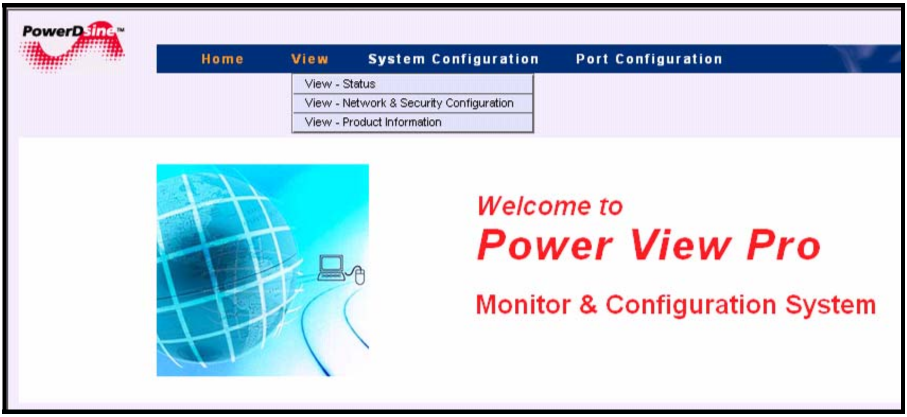


Figure 4-1: Opening Screen

4.3 View Screen

View menu – used to view the following categories (see Figure 4-2):

- Status
- Network Configuration
- Product Information



PowerDsine™
Home
View
System Configuration
Port Configuration
View - Status
View - Network & Security Configuration
View - Product Information
Welcome to
Power View Pro
Monitor & Configuration System

Figure 4-2: View Menu

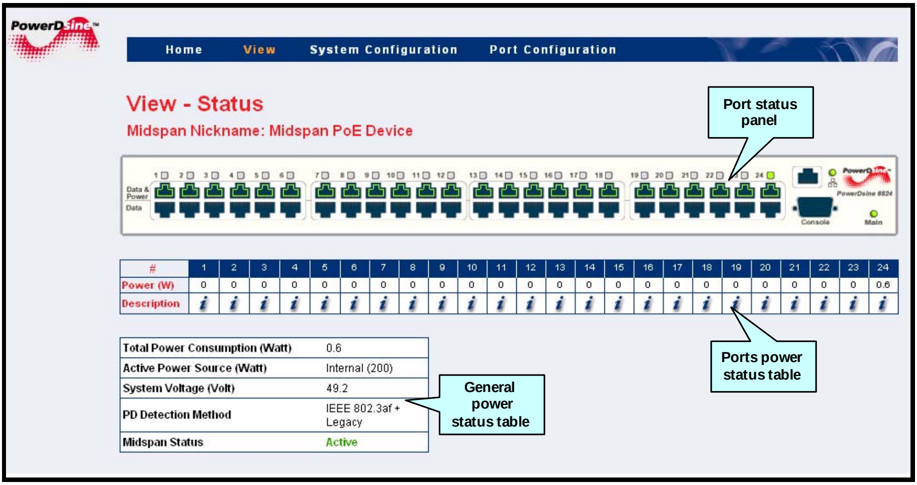
4.3.1 View Status Screen

The View Status screen is the main Midspan monitoring tool. It comprises three elements (see Figure 4-3):

- Ports status panel
- Ports power status table
- General power status table

The Ports status panel displays the following parameters:

- Ports Status
- Link Status
- AC/DC Input Power Status.



View - Status

Midspan Nickname: Midspan PoE Device

#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Power (W)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.6
Description	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i

Total Power Consumption (Watt)	0.6
Active Power Source (Watt)	Internal (200)
System Voltage (Volt)	49.2
PD Detection Method	IEEE 802.3af + Legacy
Midspan Status	Active

Figure 4-3: View Status Screen

4.3.1.1 Ports Status Panel

The display panel includes a number of visual indicators as shown in Figure 4-4; Green illuminated port indicates that the terminal unit has been identified as "Power over Ethernet Enabled" and is active and receiving power. Disabled ports illuminate red, indicating that the port is not supplying power and is not active. An "*X*" symbol appears as well.

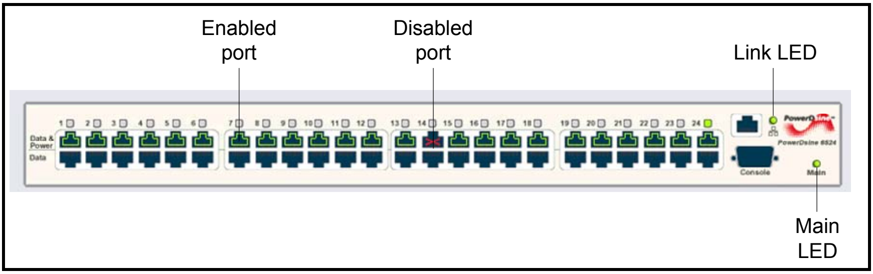


Figure 4-4: Ports Status Panel

4.3.1.2 Power & Communication Indications

Two LED's are located on the front panel, marked "Main" and Link as described in Table 4-1 and

Table **4-2**.

Table 4-1: Main Status Indications

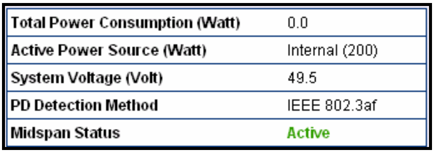
Indicator	Color	Main Power Status	Remarks
Main	Off	Internal power supply unit is unplugged.	Internal power supply voltage is too low. All ports are disconnected.
	Green	AC power input active	Internal power supply voltage is within limits.

Table 4-2: Port Status Indications

Port LED Color	Port Load Conditions	Port Voltage
Off	Inactive load or unplugged port	ver to the port is disconnected. No DC voltage present on port output lines.
Green	Active load is plugged in and complies with normal load conditions	Continuous nominal DC voltage is present on the spare pairs.
Green blinks at a 1 second rate	Overload or short circuit	Power to the port is disconnected. No DC voltage is present on port output lines.
Green blinks at a 0.5 second rate	Valid load Total aggregated power exceeds pre-defined power budget (400w by default)	Power to the port is not connected. No DC voltage is present on port output lines

4.3.1.3 Ports Power Status Table

Ports Power Status Table displays the following parameters:



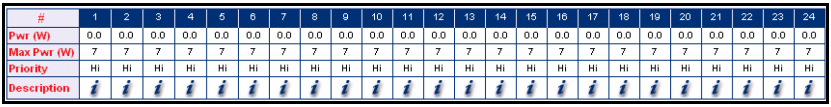
Total Power Consumption (Watt)	0.0
Active Power Source (Watt)	Internal (200)
System Voltage (Volt)	49.5
PD Detection Method	IEEE 802.3af
Midspan Status	Active

No.	Parameter	Description
1.	***Total Power Consumption***	Total power consumed by all PDs

No.	Parameter	Description
2.	***Active Power Source***	Maximum available DC power source as configured in the System Configuration - Product Parameters menu (Para. 4.4.5)
3.	***System Voltage***	Voltage level supplied to PDs
4.	***PD Detection Method***	Detection method selected by the user from the System Configuration - Product Parameters menu (see Para. 4.4.5)
5.	***Midspan Status***	Midspan status display with the following options: 1. *Active* – normal operation 2. *Midspan has no firmware* - Midspan has no firmware indication 3. *Internal Comm. Failure* – internal communication failure 4. *Midspan firmware update* - firmware update indication

4.3.1.4 General Power Status Table

General Power Status Table displays the following parameters:



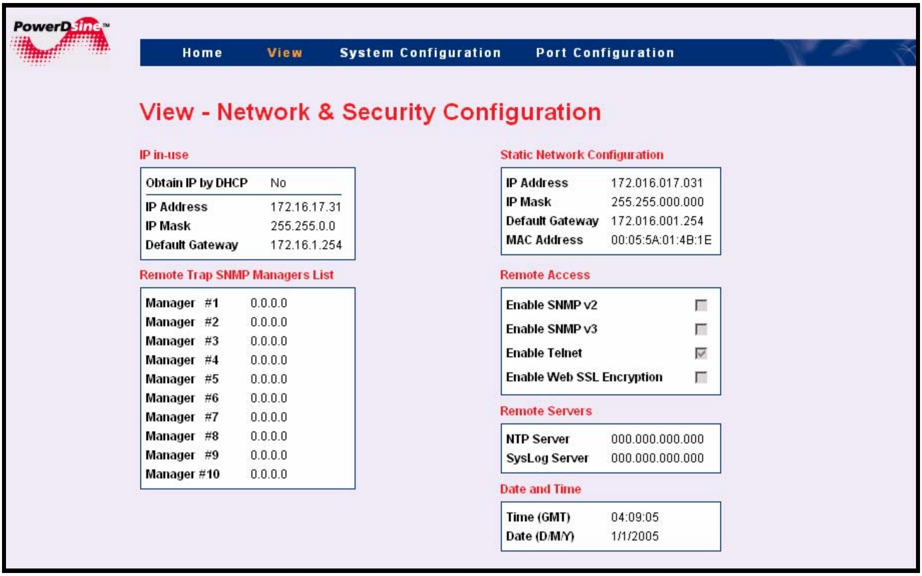
#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Pwr (W)	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Max Pwr (W)	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
Priority	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi	Hi
Description	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i

No.	Parameter	Description
1.	*PWR*	Actual consumed power by individual PD
2.	*Max Pwr*	Maximal allocated power per Port as configured in the Port Configuration – Detailed screen (see Para. 5.13)
3.	*Priority*	Current priority level set by the user
4.	*Description*	Terminal description and Terminal type as configured in the *Port Configuration – Detailed* screen (see Para. 5.13)

4.3.2 View – Network & Security Configuration Screen

View - Network Configuration Screen displays the following parameters:

- *IP in-Use* – currently used IP address/Mask/ Gateway
- *Remote Trap SNMP Managers List*- list of appointed managers
- *Static Network Configuration* – manually configured Network parameters
- *Remote Access* – Remote managers that may access the Midspan (SNMP v1/v2 and SNMPv3, Telnet) and enabled/disabled SSL WEB encryption
- *Remote Servers* – IP address of remote SysLog Server, IP address of remote NTP (Network Time Protocol) Server.
- *Date & Time* – Unit system time (GMT), as acquired from the NTP Server



View - Network & Security Configuration

IP in-use

Obtain IP by DHCP	No
IP Address	172.16.17.31
IP Mask	255.255.0.0
Default Gateway	172.16.1.254

Remote Trap SNMP Managers List

Manager #1	0.0.0.0
Manager #2	0.0.0.0
Manager #3	0.0.0.0
Manager #4	0.0.0.0
Manager #5	0.0.0.0
Manager #6	0.0.0.0
Manager #7	0.0.0.0
Manager #8	0.0.0.0
Manager #9	0.0.0.0
Manager #10	0.0.0.0

Static Network Configuration

IP Address	172.016.017.031
IP Mask	255.255.000.000
Default Gateway	172.016.001.254
MAC Address	00:05:5A:01:4B:1E

Remote Access

Enable SNMP v2	□
Enable SNMP v3	□
Enable Telnet	☑
Enable Web SSL Encryption	□

Remote Servers

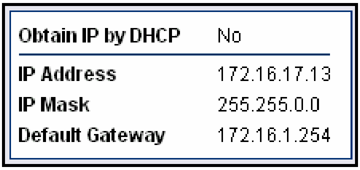
NTP Server	000.000.000.000
SysLog Server	000.000.000.000

Date and Time

Time (GMT)	04:09:05
Date (D/M/Y)	1/1/2005

4.3.2.1 IP in-Use

IP in-Use window displays the current IP address being used with the following parameters:

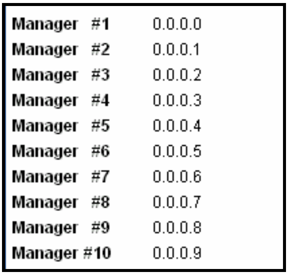


Obtain IP by DHCP	No
IP Address	172.16.17.13
IP Mask	255.255.0.0
Default Gateway	172.16.1.254

No.	Parameter	Description
1.	*Obtain IP by DHCP*	Indicates how the IP is obtained as previously set by the user (see *System Configuration – Network* - Para 5.6)*.*
2.	*IP Address*	IP address, numerical address which indicates a particular computer within a network
3.	*IP Mask*	The definition of the network portion of the IP address. This location must be configured in such a way that all IP addresses up to and including the local gateway are allowed.
4.	*Default Gateway*	The IP address of the local Gateway, which enables communication settings to other LAN segments.

4.3.2.2 Remote Trap SNMP Managers List

This List displays all the user pre-configured managers (see Para. 5.7 for further details). All listed managers receive standard and private traps from the Midspan.

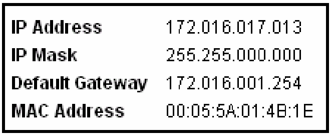


Manager #1	0.0.0.0
Manager #2	0.0.0.1
Manager #3	0.0.0.2
Manager #4	0.0.0.3
Manager #5	0.0.0.4
Manager #6	0.0.0.5
Manager #7	0.0.0.6
Manager #8	0.0.0.7
Manager #9	0.0.0.8
Manager #10	0.0.0.9

4.3.2.3 Static Network Configuration

Static Network Configuration window displays Network configuration in cases where Static IP is selected (and not DHCP). In cases where the unit is configuered as Static IP, both IP-In Use and Static configuration tables will be identical.

The following static parameters appears:

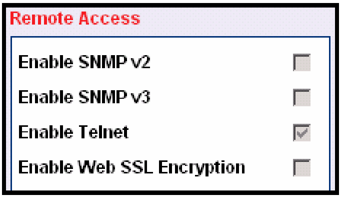


IP Address	172.016.017.013
IP Mask	255.255.000.000
Default Gateway	172.016.001.254
MAC Address	00:05:5A:01:4B:1E

No.	Parameter	Description
1.	*IP Address*	Internet address, numerical address which indicates a particular computer within a network
2.	*IP Mask*	The definition of the network portion of the IP address. This location must be configured in such a way that all IP addresses up to and including the local gateway are allowed.
3.	*Default Gateway*	IP address of the local Gateway, which enables communication settings to other LAN segments.
4.	*MAC Address*	Media access control address. A 12-digit hexadecimal address used by the media access control layer of an 802.2 connection. connection with Host Integration Server.

4.3.2.4 Remote Access

The *Remote Access* window displays the remote managers that may access the unit (SNMPv1/v2 , SNMPv3, Telnet) and enabled/disabled SSL WEB encryption.



Remote Access

Enable SNMP v2 □

Enable SNMP v3 □

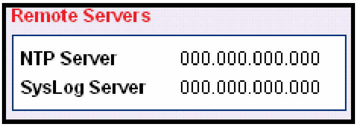
Enable Telnet ☑

Enable Web SSL Encryption □

No.	Parameter	Description
1.	Enable SNMPv2	Indicates enabled/disabled SNMP v1/v2
2.	Enable SNMPv3	Indicates enabled/disabled SNMPv3, due to security considerations. Note that it is not recommended to enable SNMPv2 while SNMPv3 is in use!
3.	Enable Telnet	When this box is checked, the user may access the unit, via the Telnet protocol.
4.	Enable Web SSL Encryption	When this box is checked, indicates that WEB pages are encrypted by SSL.

4.3.2.5 Remote Servers

Remote Servers window displays the IP address of a remote SysLog Server, and an IP address of remote NTP (Network Time Protocol) Server.



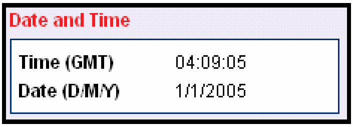
Remote Servers

NTP Server 000.000.000.000
SysLog Server 000.000.000.000

No.	Parameter	Description
1.	NTP Server	IP address of a remote Network Time Protocol (NTP) Server
2.	SysLog Server	Log Events sent to the IP address via SysLog protocol Note that an IP address 0.0.0.0 prohibits the unit from sending Log Events

4.3.2.6 Date and Time

Date and Time window displays unit system time (GMT), as acquired from the NTP Server.



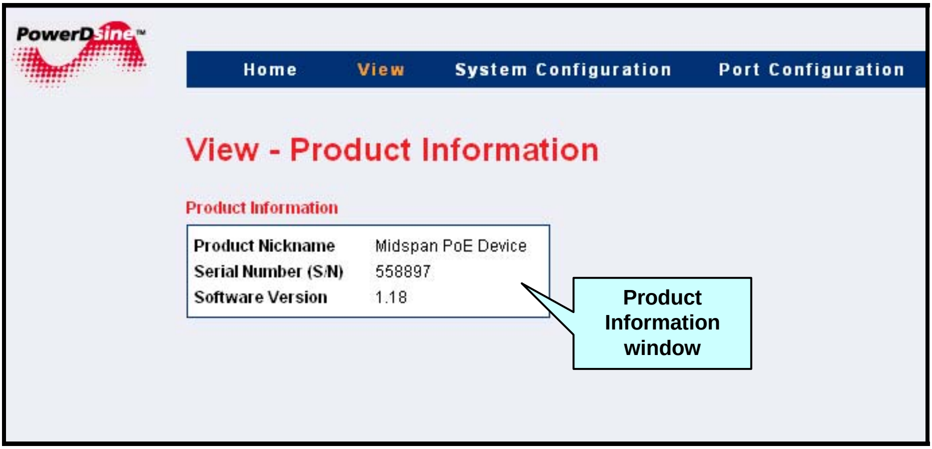
Date and Time

Time (GMT) 04:09:05
Date (D/M/Y) 1/1/2005

No.	Parameter	Description
1.	Time (GMT)	Time (HH:MM:SS) as acquired from the NTP Server
2.	Date (D/M/Y)	Date (DD/MM/YYYY) as acquired from the NTP Server If the unit fails to acquire time from the NTP Server, it will display the elapsed time since 1/2/2005

4.3.3 View - Product Information

View - Product Information screen displays the following parameters (see Figure 4-5):



View - Product Information

Product Information

Product Nickname	Midspan PoE Device
Serial Number (S/N)	558897
Software Version	1.18

Figure 4-5: View - Product Information Screen

No.	Parameter	Description
1.	*Product Nickname*	Unit nickname as configured by network administrator
2.	*Serial Number*	Midspan serial number
3.	*Software Version*	Current software version

4.4 System Configuration Screen

System Configuration Screen allows the following Configurations*:* (Figure 4-6):

- *Network Configuration*
- *SNMP Configuration*
- *SNMPv3 Configuration*
- *Security Configuration*
- *Product Parameters-Configuration*
- *System Configuration - Maintenance*

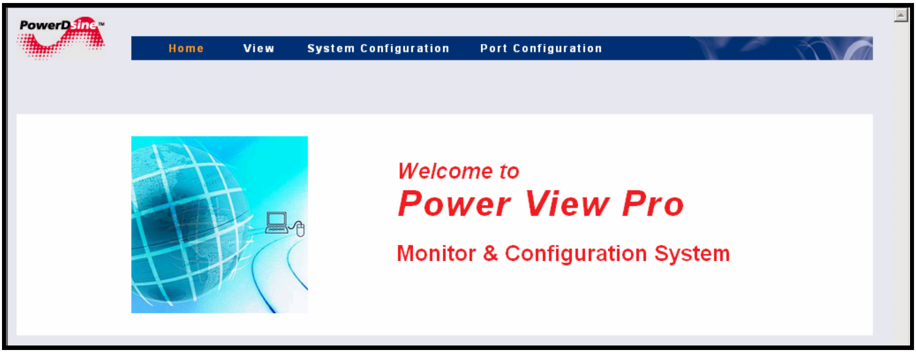
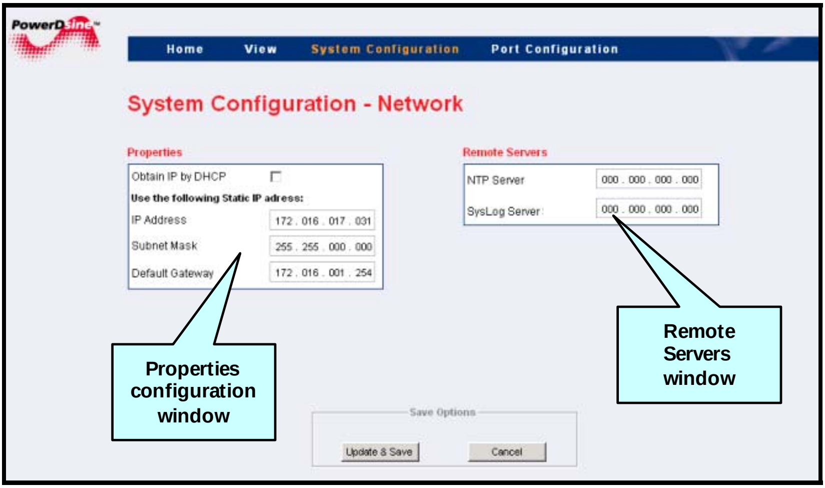


Figure 4-6: System Configuration Screen

4.4.1 System Configuration Network Screen

Network Configuration screen (see Figure 4-7) allows Configuration of the following parameters (see also para. 4.3.2.1): *IP Address, Subnet Mask, Default Gateway.*



System Configuration - Network

Properties

Obtain IP by DHCP □

Use the following Static IP adress:

IP Address 172 . 016 . 017 . 031

Subnet Mask 255 . 255 . 000 . 000

Default Gateway 172 . 016 . 001 . 254

Remote Servers

NTP Server 000 . 000 . 000 . 000

SysLog Server 000 . 000 . 000 . 000

Save Options

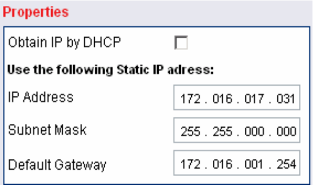
Update & Save

Cancel

Properties configuration window

Remote Servers window

Figure 4-7: System Configuration Network Screen

No.	Button/Checkbox	Description
1.		When checked enables the DHCP to obtain IP by server; Note that the *Static IP Address* fields are dimmed!
2.	 Properties Obtain IP by DHCP □ Use the following Static IP adress: IP Address 172 . 016 . 017 . 031 Subnet Mask 255 . 255 . 000 . 000 Default Gateway 172 . 016 . 001 . 254	Static IP address to be used in cases where DHCP is disabled.
3.		Static IP subnet mask to be used in cases where DHCP is disabled.
4.		Static IP default gateway to be used in cases where DHCP is disabled
5.	NTP Server	IP address of a remote NTP Server
6.	SysLog Server	IP address of a remote SysLog server to which the Midspan sends log events. Note that an IP address 0.0.0.0 prohibits the unit from sending Log

No.	Button/Checkbox	Description
		events.
7.		Updates Midspan properties status and saves configuration in cases where Midspan restarts working. All Properties and Remote Servers parameters become effective only after this button has been clicked.
8.		Cancels current operation and restores previous values in cases where the *Update & Save* buttons were not clicked.

4.4.1.1 Log Server

The Midspan can send various internal events reports to an external Host which logs those events for future use. SysLog messages are sent whenever the SysLog Server's IP is other than '0.0.0.0'. The following events may be sent by the Midspan:

- System was restarted
- PSE port SNMP status has changed
- Midspan delivers power above xy% threshold
- Midspan delivers power less then xy% threshold (after ePWR_USAGE_TO_HIGH signal was sent)
- Remote user tried to access WEB view pages using an incorrect password
- Remote user tried to access WEB configuration pages using incorrect password
- Unit's factory default values were restored
- Unit configuration was changed
- Remote Telnet user failed to login (incorrect user or password)
- Log events are being sent as SysLog messages. Syslog is a method utilized to collect messages from devices to be sent to a server running a syslog daemon. Logging to a central syslog server assists in aggregation of logs and alerts

NOTE:

Each SysLog message contains the message itself and date & time (GMT). The Midspan acquires date & time from the Network NTP Server.

4.4.1.2 NTP Server

whenever a valid NTP Server IP is configured, the Midspan acquires date & time (GMT) from the Network NTP Server. In cases where no valid IP is set, or in cases where the Midspan fails to acquire time from the NTP Server, initial Midspan time will be set to 1/1/2005 as default.

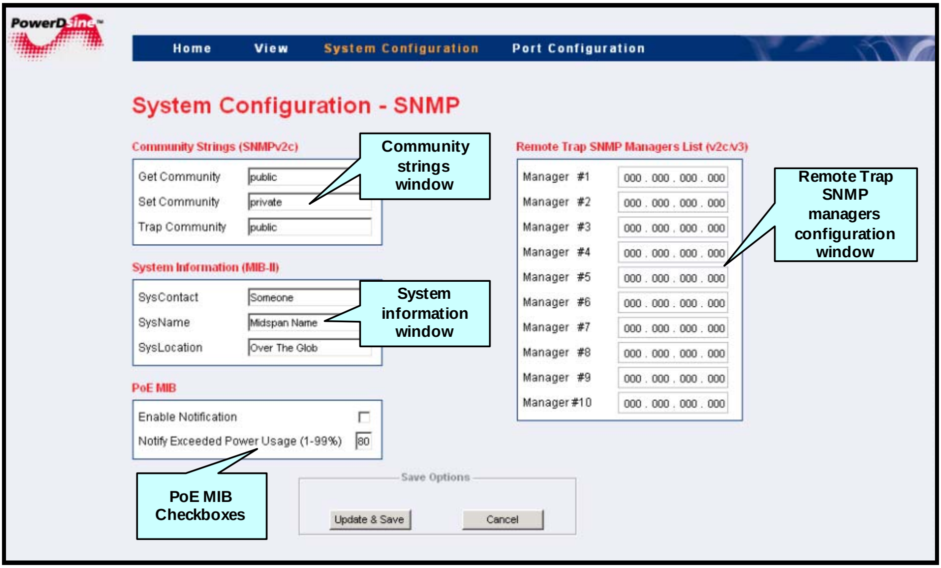
4.4.2 System Configuration SNMP

The Unit's SNMP agent (v1/v2/v3) enables remote SNMP management station to monitor a unit, enable/disable PoE ports (RFC3621), view various PoE MIB statistics and MIB-II Network statistics.

The SNMPv3 offers a secured method for configuration and monitoring. SNMP Network packets may be authenticated by MD5 and encrypted by DES.

System Configuration SNMP screen allows configuration of SNMP parameters that are common both to SNMPv1/v2 and SNMPv3 (SNMPv1/2 community string is the only exception). The following parameters can be configured (see Figure 4-8):

- *Community Strings*
- *System Information*
- *Remote Trap SNMP Managers List*



System Configuration - SNMP

Community Strings (SNMPv2c)

Get Community	public
Set Community	private
Trap Community	public

System Information (MIB-II)

SysContact	Someone
SysName	Midspan Name
SysLocation	Over The Glob

PoE MIB

Enable Notification	□
Notify Exceeded Power Usage (1-99%)	80

Remote Trap SNMP Managers List (v2c/v3)

Manager #1	000 . 000 . 000 . 000
Manager #2	000 . 000 . 000 . 000
Manager #3	000 . 000 . 000 . 000
Manager #4	000 . 000 . 000 . 000
Manager #5	000 . 000 . 000 . 000
Manager #6	000 . 000 . 000 . 000
Manager #7	000 . 000 . 000 . 000
Manager #8	000 . 000 . 000 . 000
Manager #9	000 . 000 . 000 . 000
Manager #10	000 . 000 . 000 . 000

Save Options

Community strings window

System information window

Remote Trap SNMP managers configuration window

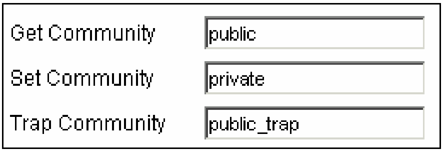
PoE MIB Checkboxes

Figure 4-8: System Configuration SNMP Screen

4.4.2.1 Community Strings (SNMPv2**c)**

Community strings are actually SNMP passwords. To enable remote SNMP manager communication with the device, the user must configure his community strings to match those of the Midspan.

Community Strings window allows configuration of the following parameters:

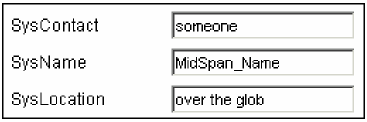


Get Community	public
Set Community	private
Trap Community	public_trap

No.	Field	Description
1.	*Get community*	Used by remote SNMP NMS station for GET commands (get information from Midspan)
2.	*Set community*	Used by remote SNMP NMS station for SET commands (change contact person, device name, etc.)
3.	*Trap community*	Each TRAP sent by the MIdspan to remote NMS managers contains Trap community string. Remote SNMP NMS managers may use it in order to filter out unnecesery TRAP events.

4.4.2.2 System Information (MIB-II)

System Information window allows configuration of the following:



SysContact someone

SysName MidSpan_Name

SysLocation over the glob

No.	Button/Checkbox	Description
1.	*SysContact*	SNMP MIB-II 1.3.6.1.2.1.1.4 : Textual identification of the contact person for this managed node, together with information on how to contact this person.
2.	*SysName*	SNMP MIB-II 1.3.6.1.2.1.1.5: Textual identification of an administratively-assigned name for current managed node
3.	*SysLocation*	SNMP MIB-II 1.3.6.1.2.1.1.6: Textual identification of the physical location of current node

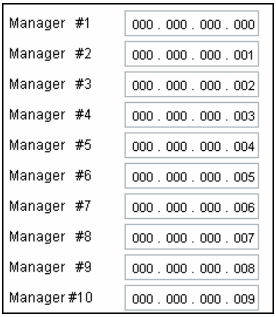
4.4.2.3 PoE MIB Checkboxes

This window allows graphical configuration of two major RFC3621 PoE MIB parameters as follows:

No.	Button/Checkbox	Description
1.	*Enable Notification*	Allows/prohibits unit from sending traps (both SNMPv2c and SNMPv3)
2.	*Notify Exceeded Power Usage (1-99%)*	The Midspan sends TRAP each time total power consumption exceeds xy%, in cases where Enable Notification checkbox is checked,

4.4.2.4 Remote Trap SNMP Managers List

This window allows configuration of up to 10 remote SNMP managers which are used by the Midspan in order to send TRAP events.

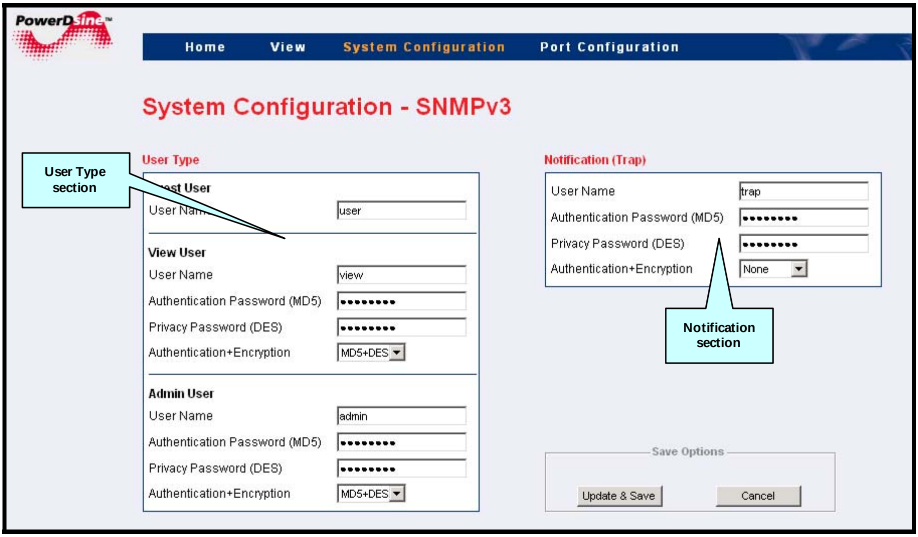


Manager #1	000 . 000 . 000 . 000
Manager #2	000 . 000 . 000 . 001
Manager #3	000 . 000 . 000 . 002
Manager #4	000 . 000 . 000 . 003
Manager #5	000 . 000 . 000 . 004
Manager #6	000 . 000 . 000 . 005
Manager #7	000 . 000 . 000 . 006
Manager #8	000 . 000 . 000 . 007
Manager #9	000 . 000 . 000 . 008
Manager #10	000 . 000 . 000 . 009

No.	Button	Description
1.	Update & Save	Updates Midspan properties status and saves configuration in cases where Midspan restarts working. All the SNMP parameters become effective only after this button has been clicked!
2.	Cancel	Cancels current operation and restores previous values

4.4.3 System Configuration SNMPv3

System Configuration SNMPv3 screen allows configuration of three different SNMPv3 user types and notification (Trap) which requires same parameters as any other SNMPv3 user.



System Configuration - SNMPv3

User Type

Guest User

User Name	user

View User

User Name	view
Authentication Password (MD5)	••••••••
Privacy Password (DES)	••••••••
Authentication+Encryption	MD5+DES

Admin User

User Name	admin
Authentication Password (MD5)	••••••••
Privacy Password (DES)	••••••••
Authentication+Encryption	MD5+DES

Notification (Trap)

User Name	trap
Authentication Password (MD5)	••••••••
Privacy Password (DES)	••••••••
Authentication+Encryption	None

Figure 4-8: System Configuration SNMPv3 Screen

- *Guest User – Allows* limited SNMPv3 user capabilities, mainly in order to use the "keep alive" poling command. The Guest user has no authentication ability or privacy (encryption).
- *View User* – Has reading (GET) access to all SNMP branches but cannot perform any modifications *(SET).*
  - *User Name* – SNMPv3 user (mandatory field)
  - *Authentication Password (MD5)* – applicable when MD5 or MD5+DES is being used.
  - *Privacy Password (DES)* – applicable only when MD5+DES is being used.

- *Authentication+Encryption – Allows selection of one of three security leveles as follows:*
  - *None* – SNMPv3 packets are not authenticated neither encrypted
  - *MD5* – SNMPv3 packets are authenticated but not encrypted
  - *MD5+DES* – SNMPv3 packets are authenticated and encrypted

- *Admin User – Has full reading (GET) and writing (SET) access to all SNMP branches*
  - *User Name* – SNMPv3 user (mandatory field)
  - *Authentication Password (MD5)* – applicable when MD5 or MD5+DES is being used.
  - *Privacy Password (DES)* – applicable only when MD5+DES is being used.
  - *Authentication+Encryption* – Allows selection of one of three security leveles:
    - *None* – SNMPv3 packets are not authenticated neither encrypted.
    - *MD5* – SNMPv3 packets are authenticated but not encrypted
    - *MD5+DES* – SNMPv3 packets are authenticated and encrypted
- *Notification Trap* – SNMPv3 trap configuration parameters are identical to SNMPv3 user
  - *User Name – SNMPv3 user (mandatory field)*
  - *Authentication Password(MD5) – applicable when MD5 or MD5+DES is being used.*
  - *Privacy Password (DES) – applicable only when MD5+DES is being used.*

- *Authentication+Encryption* – allows selection of one of three security leveles:
  - *None* – SNMPv3 packets are not authenticated and neither encrypted
  - *MD5* – SNMPv3 packets are authenticated but not encrypted
  - *MD5+DES* – SNMPv3 packets is authenticated and encrypted

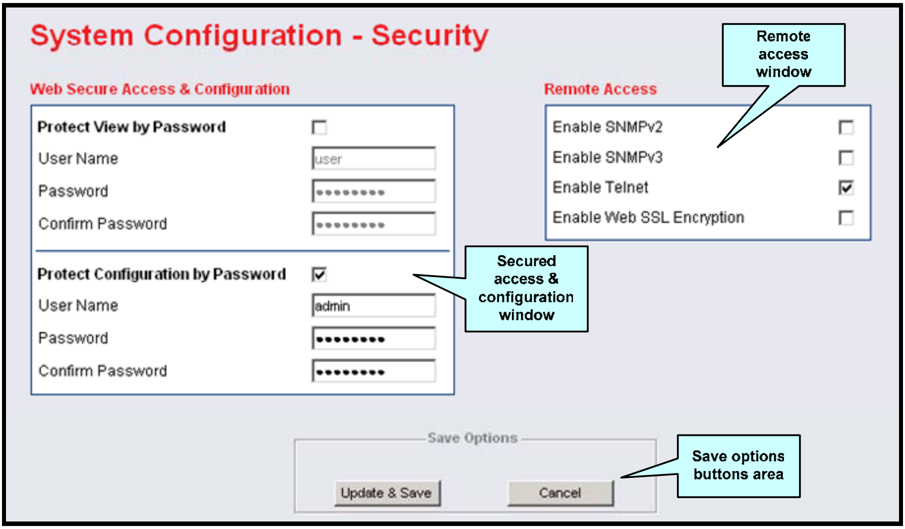
NOTE:

Notification (Trap) remote manager can be configured via the System Configuration – SNMP WEB page NTP Server.

4.4.4 System Configuration Security

System Configuration Security screen allows Configuration of the following parameters (see Figure 4-9):

- *Secure Access & Configuration*
- *Remote Access* communication type



System Configuration - Security

Web Secure Access & Configuration

Protect View by Password	□
User Name	user
Password	••••••••
Confirm Password	••••••••
Protect Configuration by Password	☑
User Name	admin
Password	••••••••
Confirm Password	••••••••

Remote Access

Enable SNMPv2	□
Enable SNMPv3	□
Enable Telnet	☑
Enable Web SSL Encryption	□

Remote access window

Secured access & configuration window

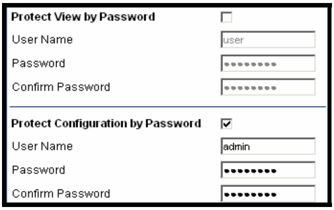
Save options buttons area

Figure 4-9: System Configuration Security Screen

4.4.4.1 Secure Access & Configuration

The user can protect one or both of the *View* and *Configuration* menus by clicking the desired appropriate checkbox; there are two types of system users as follows:

System User who is allowed to use the View menu only and System administrator who is allowed to view and use all the GUI functions. Password and user name are also set in this window and the user is prompted to type the appropriate password and user name when accessing the protected menus.

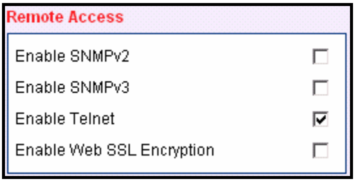


Protect View by Password	☐
User Name	user
Password	••••••••
Confirm Password	••••••••
Protect Configuration by Password	☑
User Name	admin
Password	•••••••••
Confirm Password	•••••••••

NOTE:

A remote Telnet user is requested to provide username and password, regardless of the check box selection state. Checking the *View* username & password checkbox, prevents remote Telnet user to perform any modifications. Checking *Configuration* username & password provides full access to remote Telnet user.

4.4.4.2 Remote Access



Remote Access

Enable SNMPv2	☐
Enable SNMPv3	☐
Enable Telnet	☑
Enable Web SSL Encryption	☐

Enable SNMPv2 – Enables management of the unit via remote SNMP manager station that utilizes SNMPv2c application.

Enable SNMPv3 - Enables management of the unit by remote SNMP manager station that utilizes SNMPv3 application.

NOTE:

Due to security considerations, when SNMPv3 is in use, it is recommended to disable the SNMPv2 application.

Enable Telnet - This commication is enabled by default. To disable remote Telnet commuication, uncheck the *Enable Telnet* checkbox.

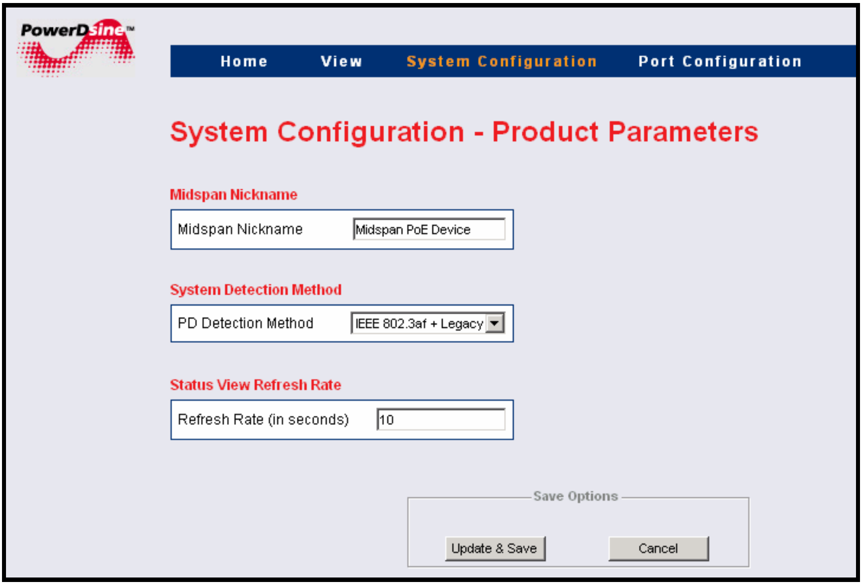
Enable Web SSL Encryption– When checked, provides security for Web pages, utilizing the SSL

No.	Button	Description
1.	Update & Save	Updates Midspan parameters and saves configuration in cases where Midspan restarts working. All Remote Access parameters become effective only after this button has been clicked.
2.	Cancel	Cancels current operation and restores previous values (in cases where Update & Save was not clicked).

4.4.5 System Configuration Product Parameters

Product parameters set by the user include (see Figure 4-10):

- *Midspan Nickname*
- *System Detection Method*
- *Status View Refresh Rate.*



System Configuration - Product Parameters

Midspan Nickname

Midspan Nickname: Midspan PoE Device

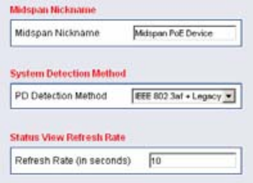
System Detection Method

PD Detection Method: IEEE 802.3af + Legacy

Status View Refresh Rate

Refresh Rate (in seconds): 10

Figure 4-10: System Configuration Product Parameters Screen

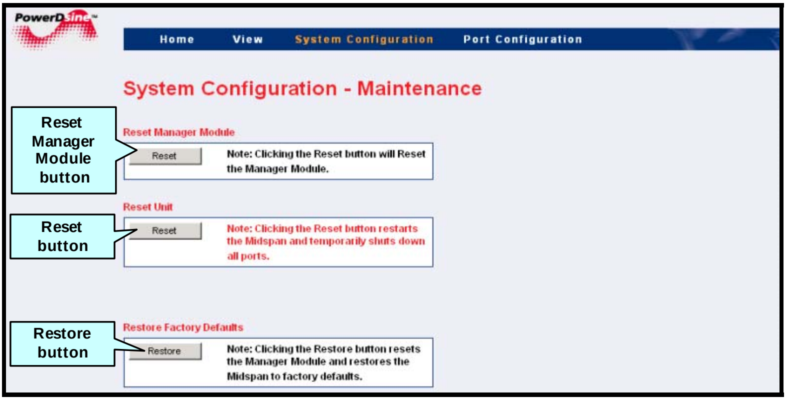
No.	Button/Checkbox	Description
1.	 Midspan Nickname Midspan Nickname: Midspan PoE Device System Detection Method PD Detection Method: IEEE 802.3af + Legacy Status View Refresh Rate Refresh Rate (in seconds): 10	Assists network managers to identify Midspan. *PD Detection Method*: *IEEE 802.3af*, or *IEEE 802.3af* +Legacy drop-down menu (*IEEE 802.3af +Legacy*=default) Allows Setting of System Status WEB page refresh rate
2.		Updates Midspan product based parameetrs. All the product parameters become effective only after this button has been clicked!
3.		Cancels current operation and restores previous values

4.4.6 System Configuration Maintenance

System Configuration Maintenance screen (see Figure 4-11) allows two maintenance means destined to maintain the Midspan.

- *Reseting the Manager Module*
- *Reseting the Midspan*
- *Restoring Factory Defaults*

When trouble is encounered, or when the Midspan does not function properly, reseting the Midspan or restoring factory default values may solve the problem.



System Configuration - Maintenance

Reset Manager Module

Note: Clicking the Reset button will Reset the Manager Module.

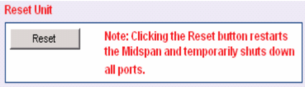
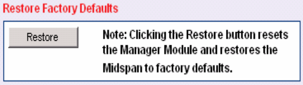
Reset Unit

Note: Clicking the Reset button restarts the Midspan and temporarily shuts down all ports.

Restore Factory Defaults

Note: Clicking the Restore button resets the Manager Module and restores the Midspan to factory defaults.

Figure 4-11: System Configuration Maintenance Screen

No.	Button/Checkbox	Description
1.	 Reset Manager Module Reset Note: Clicking the Reset button will Reset the Manager Module.	Resets only the Manager Module without affecting Midspan PoE ports
2.	 Reset Unit Reset Note: Clicking the Reset button restarts the Midspan and temporarily shuts down all ports.	Resets unit temporarily. All active PoE ports momentarely stop providing Power to PoE devices (configuration does not change)
3.	 Restore Factory Defaults Restore Note: Clicking the Restore button resets the Manager Module and restores the Midspan to factory defaults.	Restore most Midspan parameters to their default value

4.5 Port Configuration Screen

Port Configuration screen allows the following (Figure 4-12):

- Port Configuration Enable/Disable
- Port Configuration Detailed

Port Configuration Enable/Disable screen provides a quick access to ports in order to Enable/Disable one or more of them.

Port Configuration Detailed screen allows detailed Configuration of various system values such as priority, allocated power and port/PD description.

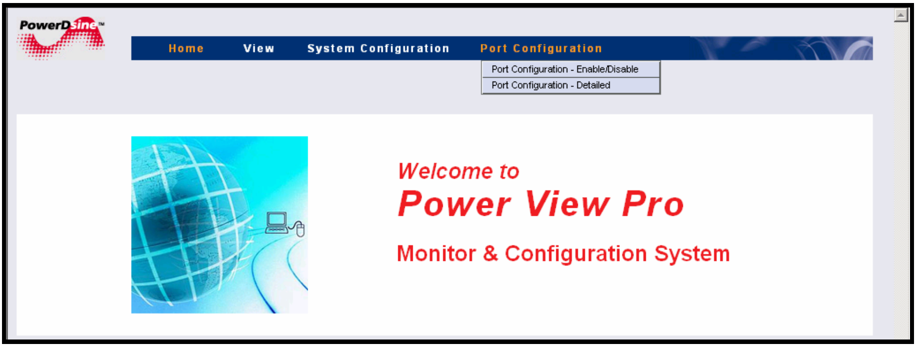
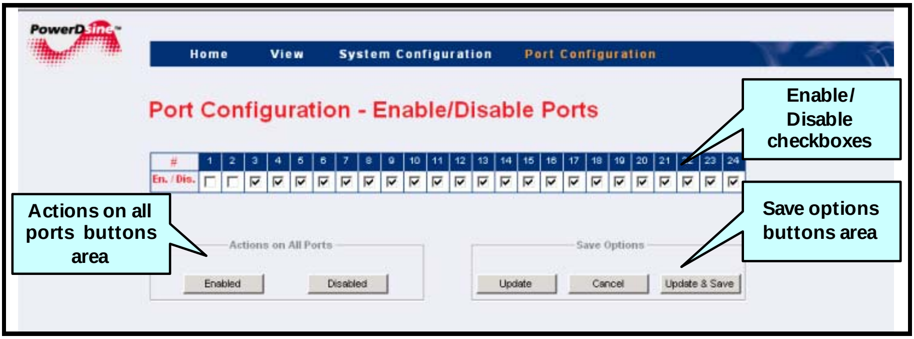

PowerDsine™
Home
View
System Configuration
Port Configuration
Port Configuration - Enable/Disable
Port Configuration - Detailed
Welcome to
Power View Pro
Monitor & Configuration System

Figure 4-12: Port Configuration Screen

4.5.1 Port Configuration Enable/Disable

Each port may be individually Enabled/Disabled, or all ports may be enabled or disabled in one action.

Once the ports are disabled, the Midspan *View Status* screen is updated accordingly (see Para. 4.3 / Figure 4-3).



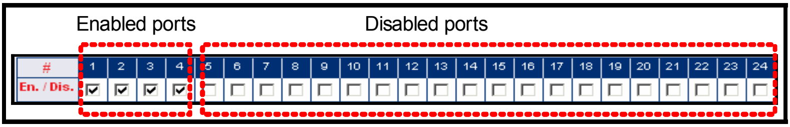
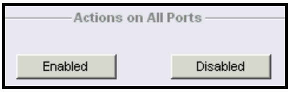
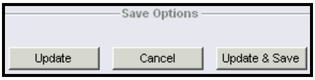


Figure 4-13: Port Configuration Enable/Disable Screen

No.	Button/Checkbox	Description
1.	 Actions on All Ports Enabled Disabled	*Enabled* – enables all ports *Disabled* - disables all ports
2.	 Save Options Update Cancel Update & Save	*Update* – Clicking this button, activates the new user settings but does not store new configuration (unit reset overides latest changes) *Cancel* – Cancels current operation and restores previous

No.	Button/Checkbox	Description
		values in cases where *Update&Save* were not clicked *Update & Save* – Updates Midspan properties status and saves configuration in cases where Midspan restarts.

NOTE:

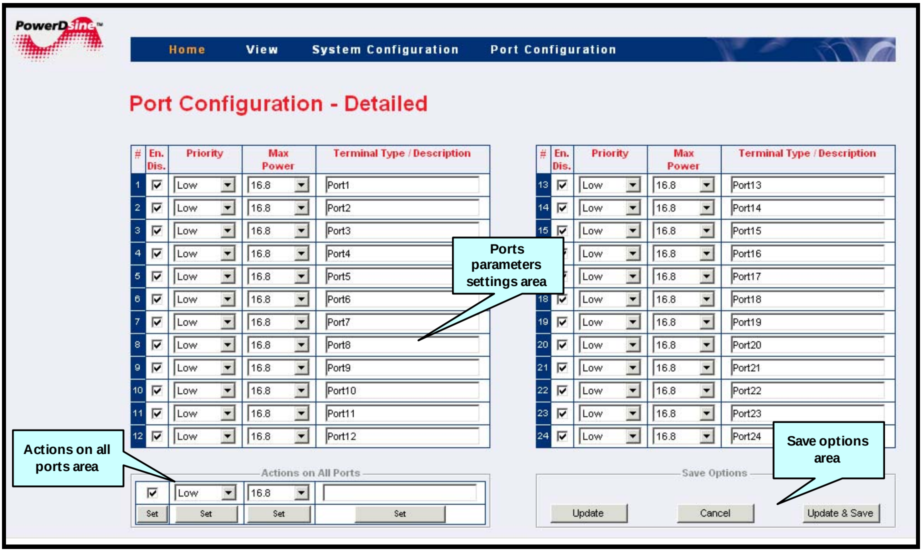
If only *update* button is pressed, a blinking image appears near the *Save & update* button, reminding the user that latest changes were not saved. Reversing latest changes and pressing *Update,* eliminates the blinking image. Saving latest changes eliminates this image as well.

4.5.2 Port Configuration Detailed

The *Port Configuration Detailed* screen (see Figure 4-14) allows the user to control individual ports and set-up parameters as follows:

- Activate/shut-down individual ports
- Allocate Maximal power per port
- Set-up the priority of each port
- Define port description and Terminal type

In order to simplify the configuration of multiple ports, each parameter may be set by pressing a single button (*SET*), thus applying the selected values to all ports (*action on all ports*).



Port Configuration - Detailed

#	En. Dis.	Priority	Max Power	Terminal Type / Description
1	☑	Low	16.8	Port1
2	☑	Low	16.8	Port2
3	☑	Low	16.8	Port3
4	☑	Low	16.8	Port4
5	☑	Low	16.8	Port5
6	☑	Low	16.8	Port6
7	☑	Low	16.8	Port7
8	☑	Low	16.8	Port8
9	☑	Low	16.8	Port9
10	☑	Low	16.8	Port10
11	☑	Low	16.8	Port11
12	☑	Low	16.8	Port12

#	En. Dis.	Priority	Max Power	Terminal Type / Description
13	☑	Low	16.8	Port13
14	☑	Low	16.8	Port14
15	☑	Low	16.8	Port15
16	☑	Low	16.8	Port16
17	☑	Low	16.8	Port17
18	☑	Low	16.8	Port18
19	☑	Low	16.8	Port19
20	☑	Low	16.8	Port20
21	☑	Low	16.8	Port21
22	☑	Low	16.8	Port22
23	☑	Low	16.8	Port23
24	☑	Low	16.8	Port24

Actions on All Ports

☑	Low	16.8	
Set	Set	Set	Set

Ports parameters settings area

Actions on all ports area

Save options area

Figure 4-14: Port Configuration Detailed Screen

4.5.2.1 Ports Activation

Ports activation/deactivation is performed by the user according to actual requirements. Each port can be switched to *Enable* or *Disable* state.

This is simply done by checking the colored checkboxes on the left hand side of the screen.

4.5.2.2 Allocating Maximum Power

Power allocation is performed by selecting the maximum allowed power per port from the drop-down menu, located on the *Max. Power* column. Available power values are as folllows:

- *Default: 16.8 W*
- *Minimum: 1 W*
- *Maximum: 16.8 W*

4.5.2.3 Setting Priority

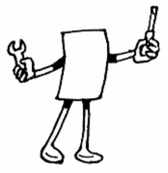
The user can assign priorities to desired PDs in cases where the Midspan is operating with a limited source of power. Priority selection is performed from the drop-down menu, located on the *Priority* column; Three priority states are available:

- *Critical*
- *High*
- *Low* (default)

The Midspan allocates all available power to the PDs, according to the PoE ports sequential number. If power consumption is exceeded, the unit enters its Power Management mode (providing power to high priority ports). Under this mode, ports having higher priority, provide power to their respective PDs.

4.5.2.4 Terminal Type / Description

In this column, the operator can enter any free text such as: terminal location, name of user, telephone No., etc. representing the corresponding port (default=Port x). Note that it has no effect on power itslelf and it functions as an assistence tool for the IT manager.



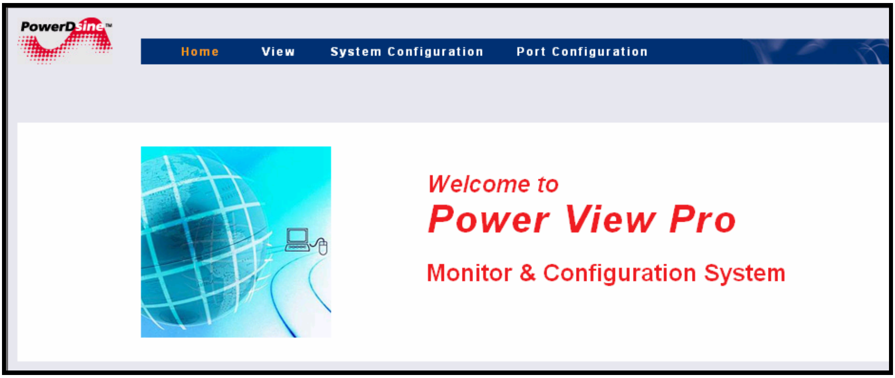
5 Operation

5.1 General

To manage multiple Midspan devices it is recommended to use 3rd party standard Network management tools such as HP Openview or SNMPc.

5.2 Logging in

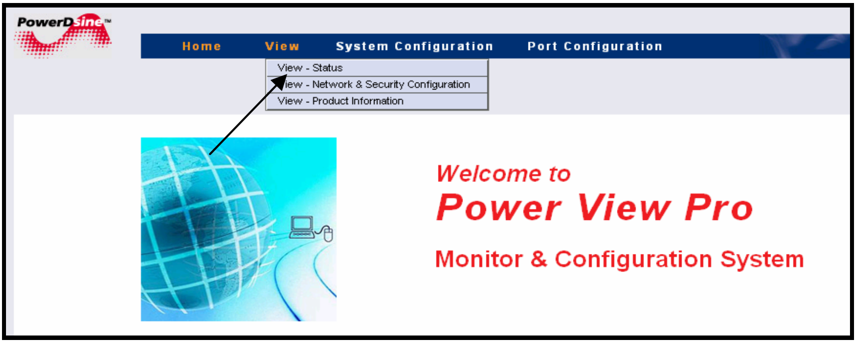
1. Verify that the RJ-45 Ethernet cable running between the PoE unit and the local area network is connected.
2. Open your Web browser and type the IP Address of the PoE unit to be managed.
3. The Main menu GUI window appears;



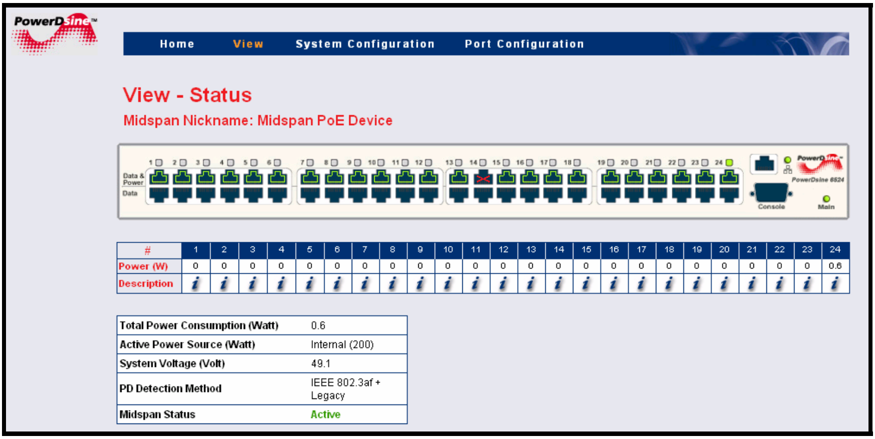
5.3 Viewing System Status

➢ To view system status:

1 Select the *View –Status* option from the *View* dropdown menu;


Home
View
System Configuration
Port Configuration
View - Status
View - Network & Security Configuration
View - Product Information
Welcome to
Power View Pro
Monitor & Configuration System

2 **View –Status** screen appears: the port status panel displays the current status. Note that in the example, Ports 1, 2 are disabled. The middle table displays power status and priority and the description raw displays the terminal type and description when the cursor points at the “I” symbol.



View - Status

Midspan Nickname: Midspan PoE Device

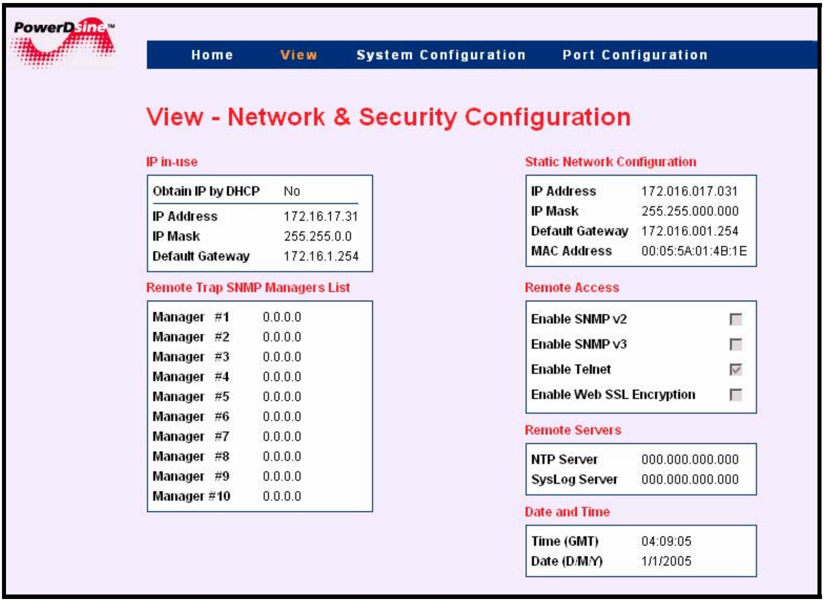
#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Power (W)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.6
Description	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i

Total Power Consumption (Watt)	0.6
Active Power Source (Watt)	Internal (200)
System Voltage (Volt)	49.1
PD Detection Method	IEEE 802.3af + Legacy
Midspan Status	Active

5.4 Viewing Network & Security Configuration Status

➢ To view Network Configuration status:

1 Select the ***View – Configuration*** option from the ***View*** dropdown menu; ***View – Configuration*** screen appears, displaying various network parameters as shown below:



View - Network & Security Configuration

IP in-use

Obtain IP by DHCP	No
IP Address	172.16.17.31
IP Mask	255.255.0.0
Default Gateway	172.16.1.254

Remote Trap SNMP Managers List

Manager #1	0.0.0.0
Manager #2	0.0.0.0
Manager #3	0.0.0.0
Manager #4	0.0.0.0
Manager #5	0.0.0.0
Manager #6	0.0.0.0
Manager #7	0.0.0.0
Manager #8	0.0.0.0
Manager #9	0.0.0.0
Manager #10	0.0.0.0

Static Network Configuration

IP Address	172.016.017.031
IP Mask	255.255.000.000
Default Gateway	172.016.001.254
MAC Address	00:05:5A:01:4B:1E

Remote Access

Enable SNMP v2	☐
Enable SNMP v3	☐
Enable Telnet	☑
Enable Web SSL Encryption	☐

Remote Servers

NTP Server	000.000.000.000
SysLog Server	000.000.000.000

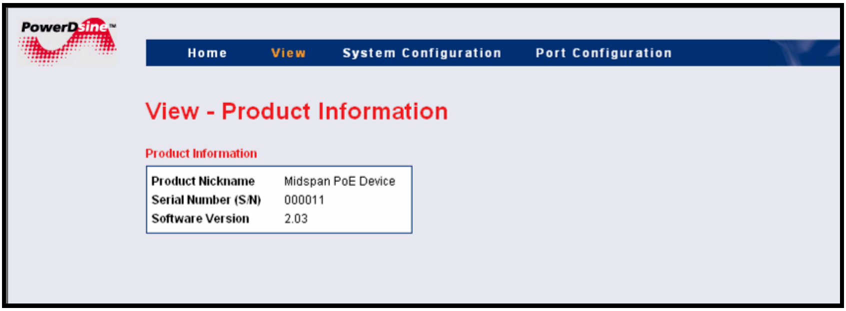
Date and Time

Time (GMT)	04:09:05
Date (D/M/Y)	1/1/2005

5.5 Viewing Product Information

➢ To view Product Information:

1 Select the ***Product Information*** option from the ***View*** dropdown menu; ***View – Product*** *Information* screen appears, displaying Product Information as shown below:



View - Product Information

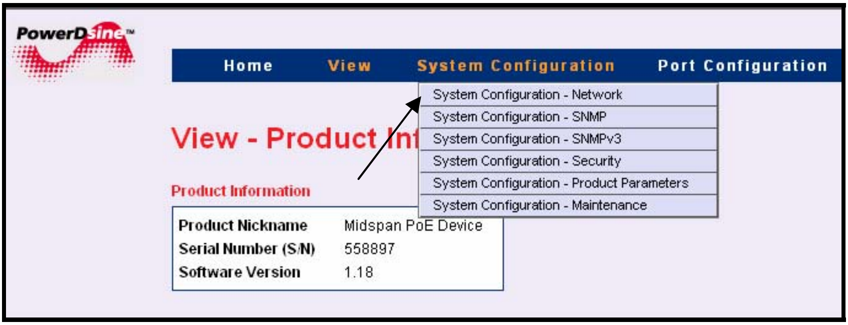
Product Information

Product Nickname	Midspan PoE Device
Serial Number (S/N)	000011
Software Version	2.03

5.6 Configuring System - Network

➢ To access System Configuration – Network:

1 Select the ***System Configuration- Network*** option from the ***System Configuration*** dropdown menu;



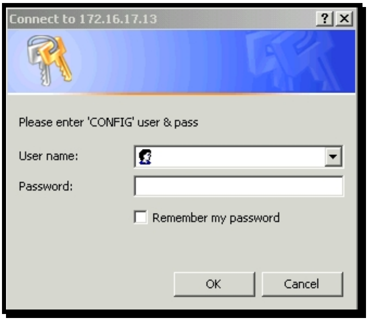
Home
View
System Configuration
Port Configuration
System Configuration - Network
System Configuration - SNMP
System Configuration - SNMPv3
System Configuration - Security
System Configuration - Product Parameters
System Configuration - Maintenance

View - Product Inf

Product Information

Product Nickname	Midspan PoE Device
Serial Number (S/N)	558897
Software Version	1.18

2 User authentication window appears:



Connect to 172.16.17.13

Please enter 'CONFIG' user & pass

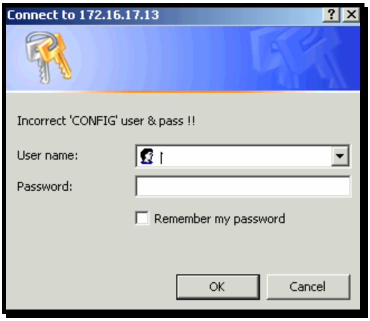
User name:

Password:

□ Remember my password

3 Type in the appropriate User name ("*admin*") and password ("*password*") and then click OK.

4 if an incorrect User name and/or password have been typed, the following message appears, prompting the user to conduct another attempt to log in.



Connect to 172.16.17.13

Incorrect 'CONFIG' user & pass !!

User name:

Password:

□ Remember my password

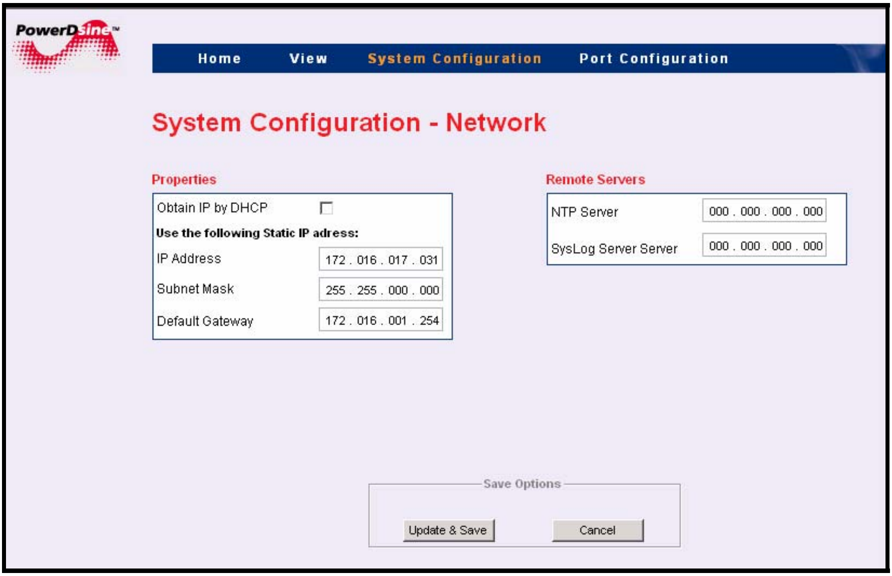
NOTE:

Three unsuccessful attempts to log in cause the application to close and the following message appears:

*"**Your Authentication failed Your Request was denied. You do not have permission to view this page**".*

To log in again, exit the program and try again.

5 *System Configuration* screen appears when logged in:



System Configuration - Network

Properties

Obtain IP by DHCP □

Use the following Static IP adress:

IP Address 172 . 016 . 017 . 031

Subnet Mask 255 . 255 . 000 . 000

Default Gateway 172 . 016 . 001 . 254

Remote Servers

NTP Server 000 . 000 . 000 . 000

SysLog Server Server 000 . 000 . 000 . 000

6 Set your desired ***IP Address, Subnet Mask*** **and** ***Default Gateway*** or check the ***Obtain IP by DHCP*** checkbox (if desired).

7 Click Update & Save to save your selection.

8 Clicking Cancel at any stage of the configuration, returns the previous value.

➢ To configure NTP Server:

1 Select the ***System Configuration***- ***Network*** option from the ***System Configuration*** dropdown menu.

2 Enter the IP address of the remote NTP Server.

➢ To configure SysLog Server:

1 Select the ***System Configuration***- ***Network*** option from the ***System Configuration*** dropdown menu.

2 Enter the IP address of the remote SysLog Server.

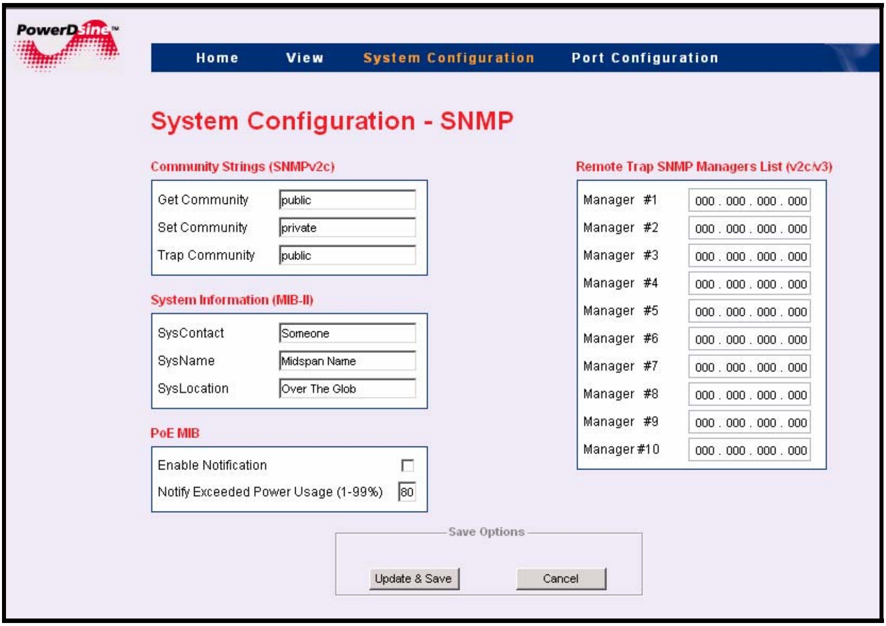
NOTE:

In order to receive Midspan Log events, please use your preferred SysLog Server application. For example:
Kiwi Syslog Daemon, via http://www.kiwisyslog.com/ , or any other SysLog Server application that comply with RFC 3164*.*

5.7 Configuring System SNMP

1 Select the ***System Configuration- SNMP*** option from the ***System Configuration*** dropdown menu;

2 ***SNMP*** window appears:



System Configuration - SNMP

Community Strings (SNMPv2c)

Get Community	public
Set Community	private
Trap Community	public

System Information (MIB-II)

SysContact	Someone
SysName	Midspan Name
SysLocation	Over The Glob

PoE MIB

Enable Notification	□
Notify Exceeded Power Usage (1-99%)	80

Remote Trap SNMP Managers List (v2c/v3)

Manager #1	000 . 000 . 000 . 000
Manager #2	000 . 000 . 000 . 000
Manager #3	000 . 000 . 000 . 000
Manager #4	000 . 000 . 000 . 000
Manager #5	000 . 000 . 000 . 000
Manager #6	000 . 000 . 000 . 000
Manager #7	000 . 000 . 000 . 000
Manager #8	000 . 000 . 000 . 000
Manager #9	000 . 000 . 000 . 000
Manager #10	000 . 000 . 000 . 000

3 Set your desired ***Community Strings***, ***System Information*** and *check the desired* option ('Enable Notification' or 'Notify Exceeded Power Usage').

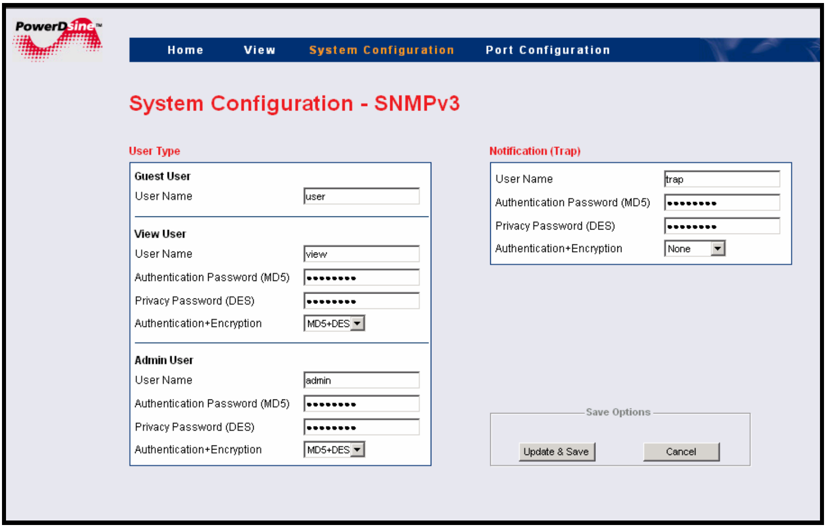
4 Click Update & Save to save your selection.

5 Clicking Cancel at any configuration stage, restores the previous value.

5.8 Configuring System SNMPv3

1 Select the ***System Configuration- SNMPv3*** option from the ***System Configuration*** dropdown menu;

2 ***SNMPv3*** window appears:



System Configuration - SNMPv3

User Type

Guest User

User Name	user

View User

User Name	view
Authentication Password (MD5)	••••••••
Privacy Password (DES)	••••••••
Authentication+Encryption	MD5+DES

Admin User

User Name	admin
Authentication Password (MD5)	••••••••
Privacy Password (DES)	••••••••
Authentication+Encryption	MD5+DES

Notification (Trap)

User Name	trap
Authentication Password (MD5)	••••••••
Privacy Password (DES)	••••••••
Authentication+Encryption	None

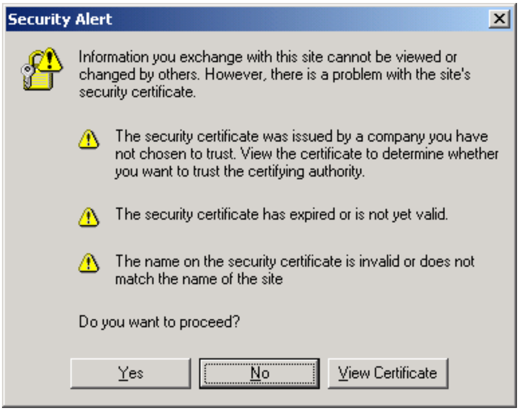
2 Fill in your desired ***Guest User***, ***View User Admin User*** and ***Notification (Trap)*** in the appropriate fields.

3 Click Update & Save to save your selection.

4 Clicking Cancel at any stage of the configuration, returns the previous value.

5.9 Configuring System Security

1 Select the ***System Configuration- Security*** option from the ***System Configuration*** dropdown menu; ***System Configuration- Security*** window appears:



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

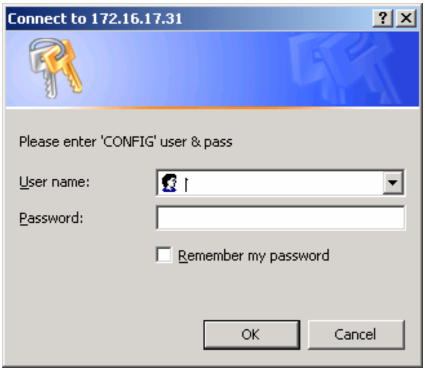
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate has expired or is not yet valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

2 Click **Yes** to continue or **No** to abort current operation: the following screen appears:



Connect to 172.16.17.31

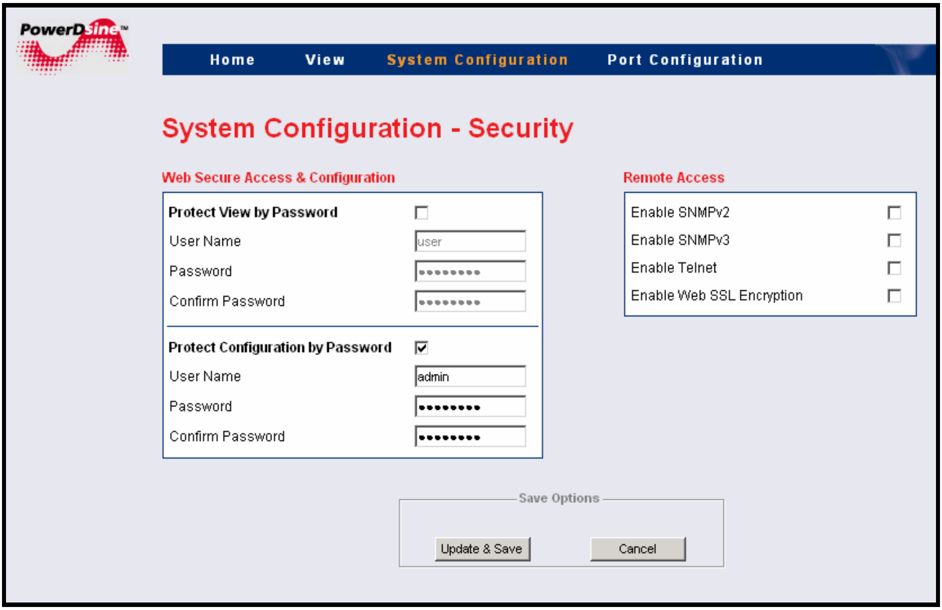
Please enter 'CONFIG' user & pass

User name:

Password:

□ Remember my password

3 Type in the appropriate User name and password; when done, click Ok to confirm: the following screen appears:



System Configuration - Security

Web Secure Access & Configuration

Protect View by Password	□
User Name	user
Password	••••••••
Confirm Password	••••••••
Protect Configuration by Password	☑
User Name	admin
Password	••••••••
Confirm Password	••••••••

Remote Access

Enable SNMPv2	□
Enable SNMPv3	□
Enable Telnet	□
Enable Web SSL Encryption	□

5.9.1 Protecting View by Password

1 Check the Protect View by Password checkbox.

2 Type in your desired Password and user name in the *Password* and *Confirm Password* fields.

3 Click Update & Save to save your selection.

4 Clicking Cancel at any stage of the configuration process, returns the previous value.

NOTE:

Password, User Name and *Confirm Password* fields are dimmed by default (can not be configured) as long as their corresponding checkbox is not checked.

5.9.2 Modifying Remote Access

1 Check the desired checkbox in the Remote Access section.

2 Click Update & Save to save your selection.

3 Clicking Cancel at any stage of the configuration, returns the previous value.

5.9.2.1 Enabling Web SSL Encryption

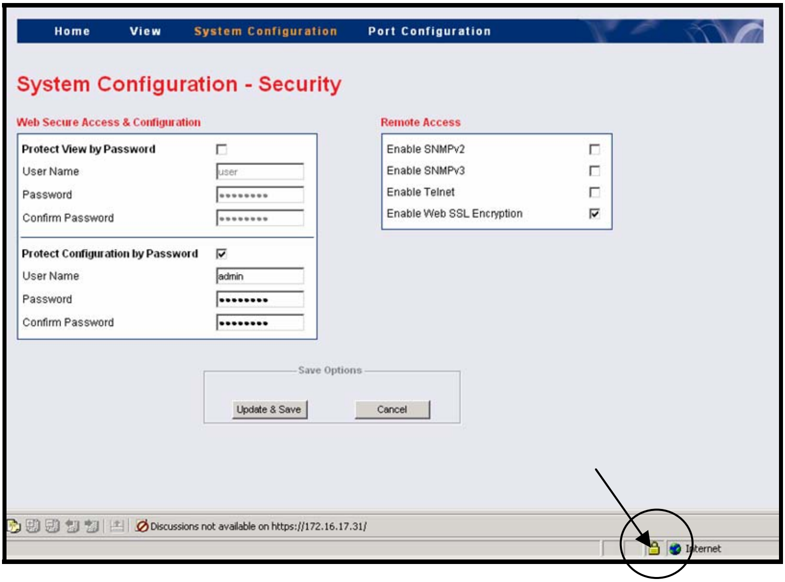
To enable Web SSL Encryption perform the following steps:

4 Check the Enable Web SSL Encryption checkbox.

5 Click Update & Save to save your selection (or Cancel to abort current operation): the following screen appears displaying a security icon at the bottom of the screen:

Note that the URL has also changed ('s' added), for example:

https://172.16.17.31/web/config/cfg_security.htm



System Configuration - Security

Web Secure Access & Configuration

Protect View by Password	☐
User Name	user
Password	••••••••
Confirm Password	••••••••
Protect Configuration by Password	☑
User Name	admin
Password	••••••••
Confirm Password	••••••••

Remote Access

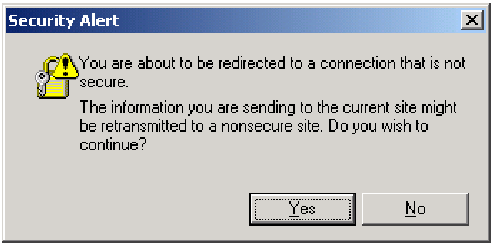
Enable SNMPv2	☐
Enable SNMPv3	☐
Enable Telnet	☐
Enable Web SSL Encryption	☑

Discussions not available on https://172.16.17.31/

5.9.2.2 Disabling Web SSL Encryption

To disable Web SSL Encryption perform the following steps:

1. Uncheck the Enable Web SSL Encryption checkbox.
2. Click Update & Save to save your selection: the following screen appears, warning the user that Web pages transmitted from this point on, are not secured:



Security Alert

You are about to be redirected to a connection that is not secure.

The information you are sending to the current site might be retransmitted to a nonsecure site. Do you wish to continue?

3. Click **Yes** to continue or **No** to abort current operation.
4. Note that the URL has also changed ('s' deleted), for example:

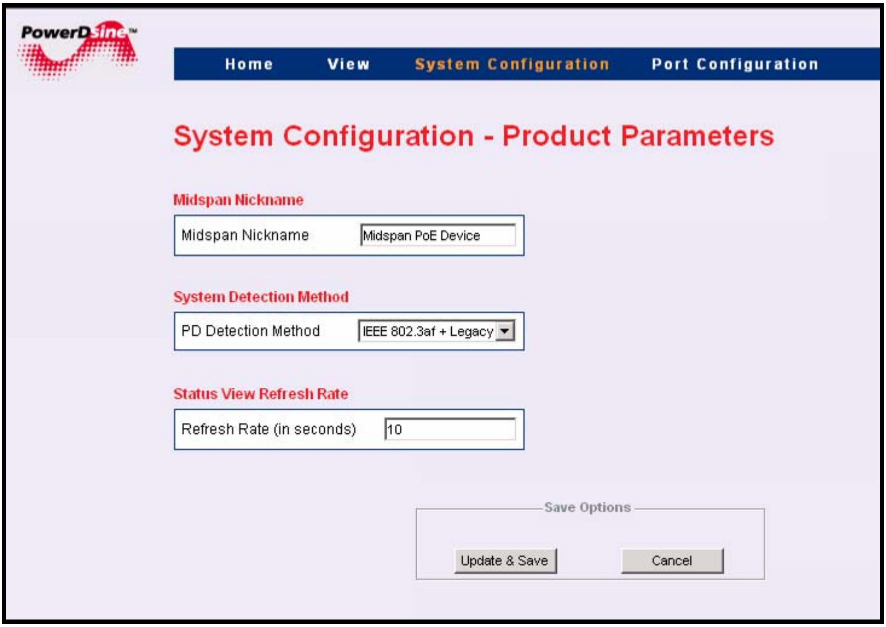
instead of:

```
https://172.16.17.31/web/config/cfg_security.htm

http://172.16.17.31/web/config/cfg_security.htm
```

5.10 Configuring Product Parameters

1 Select the ***System Configuration- Product Parameters*** option from the **System Configuration** dropdown menu;

2 ***System Configuration- Product Parameters*** window appears:



System Configuration - Product Parameters

Midspan Nickname

Midspan Nickname: Midspan PoE Device

System Detection Method

PD Detection Method: IEEE 802.3af + Legacy

Status View Refresh Rate

Refresh Rate (in seconds): 10

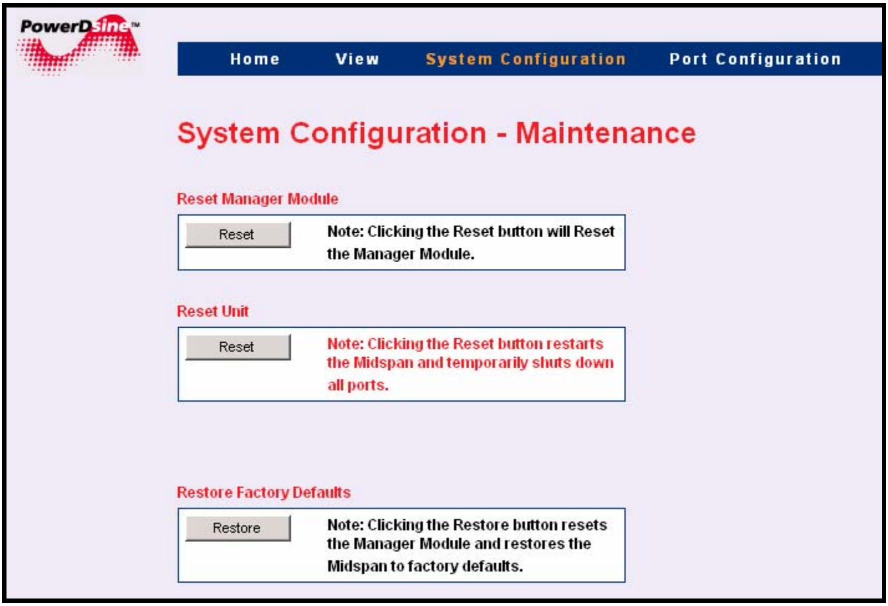
6 Type in your desired ***Midspan Nickname*** *and* ***System Detection Method*** and ***Status View Refresh Rate***.

7 Click Update & Save to save your selection.

8 Clicking Cancel at any stage of the configuration process, returns the previous value.

5.11 Configuring System Maintenance

1 Select the ***System Configuration- Maintenance*** option from the **System Configuration** dropdown menu; ***System Configuration- Maintenance*** window appears:



System Configuration - Maintenance

Reset Manager Module

Note: Clicking the Reset button will Reset the Manager Module.

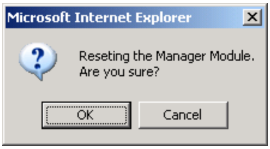
Reset Unit

Note: Clicking the Reset button restarts the Midspan and temporarily shuts down all ports.

Restore Factory Defaults

Note: Clicking the Restore button resets the Manager Module and restores the Midspan to factory defaults.

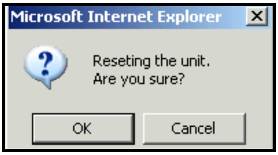
2 Click the Reset to reset down the Manager Module; the following message appears



Reseting the Manager Module.
Are you sure?

3 Click *OK* to confirm reset or *Cancel* to abort current operation.

4 Click the Reset to shut down the unit and restart again; the following message appears:

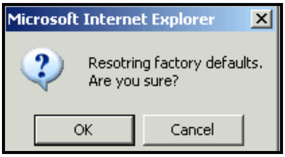


Microsoft Internet Explorer

Reseting the unit.
Are you sure?

5 Click *OK* to confirm reset or *Cancel* to abort current operation.

6 Click the Restore to restore factory defaults. The following message appears:



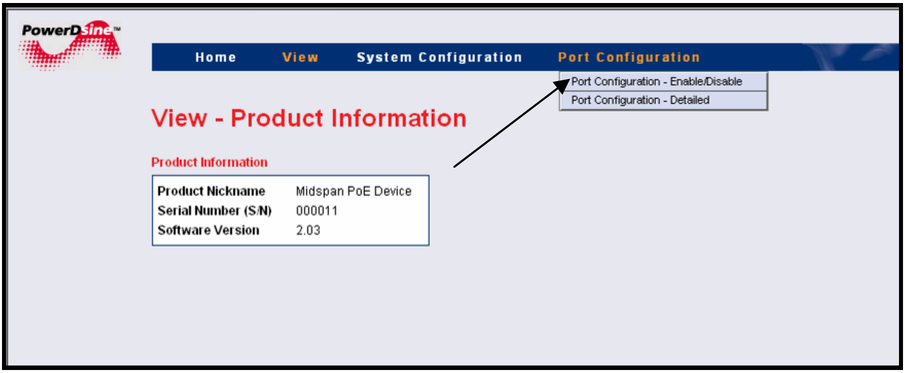
Microsoft Internet Explorer

Resotring factory defaults.
Are you sure?

7 Click *OK* to confirm reset or *Cancel* to abort current operation.

5.12 Configuring the Ports

1 Select the ***Port Configuration- Enable/Disable*** option from the ***Port Configuration*** dropdown menu;



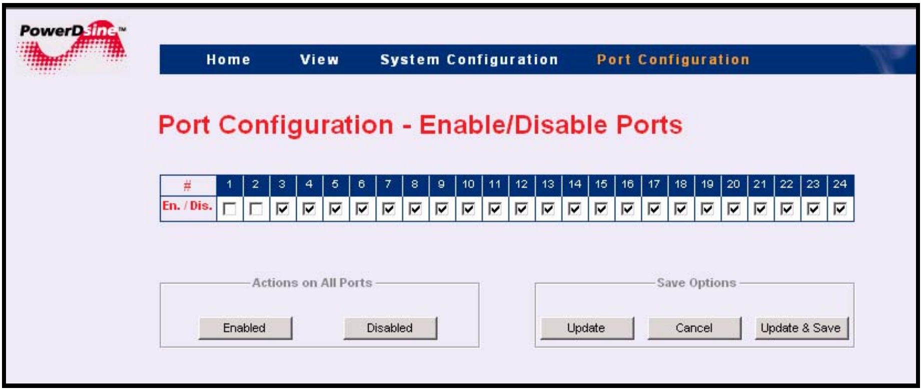
Home
View
System Configuration
Port Configuration
Port Configuration - Enable/Disable
Port Configuration - Detailed

View - Product Information

Product Information

Product Nickname	Midspan PoE Device
Serial Number (S/N)	000011
Software Version	2.03

2 ***Port Configuration- Enable/Disable*** window appears:



Port Configuration - Enable/Disable Ports

#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
En. / Dis.	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

3 Check the corresponding checkboxes to enable your desired ports.

4 Uncheck the corresponding checkboxes to disable your desired ports.

5 Click the Enabled or Disabled buttons to enable/ disable all ports at once.

6 Click Update to update the configured port status, or Cancel to abort operation and return to previous values.

NOTE:

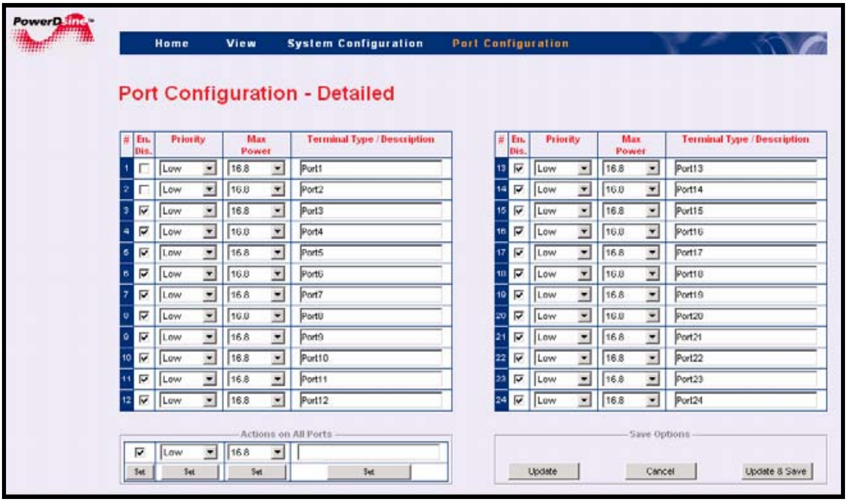
The Save starts flashing if Update is clicked, prompting the user to save the modified configuration.

7 Click Update & Save to update and save the configured port status; Midspan configuration is updated accordingly.

5.13 Configuring Additional Port Settings

1 Select the ***Port Configuration- Detailed*** option from the **Port Configuration** dropdown menu;

2 ***Port Configuration- Detailed*** window appears:



Port Configuration - Detailed

#	En. Dis.	Priority	Max Power	Terminal Type / Description
1	☐	Low	16.8	Port1
2	☐	Low	16.8	Port2
3	☑	Low	16.8	Port3
4	☑	Low	16.8	Port4
5	☑	Low	16.8	Port5
6	☑	Low	16.8	Port6
7	☑	Low	16.8	Port7
8	☑	Low	16.8	Port8
9	☑	Low	16.8	Port9
10	☑	Low	16.8	Port10
11	☑	Low	16.8	Port11
12	☑	Low	16.8	Port12

#	En. Dis.	Priority	Max Power	Terminal Type / Description
13	☑	Low	16.8	Port13
14	☑	Low	16.8	Port14
15	☑	Low	16.8	Port15
16	☑	Low	16.8	Port16
17	☑	Low	16.8	Port17
18	☑	Low	16.8	Port18
19	☑	Low	16.8	Port19
20	☑	Low	16.8	Port20
21	☑	Low	16.8	Port21
22	☑	Low	16.8	Port22
23	☑	Low	16.8	Port23
24	☑	Low	16.8	Port24

Actions on All Ports

☑	Low	16.8	
Set	Set	Set	Set

Save Options

5.13.1 Specific Ports Settings

1 Access each ports parameters individually: set the desired ***Enabled/Disables*** **status,** ***Priority, Max. Power, Terminal Type*** and ***Description***.

2 Click Update to update the configured parameters, or Cancel to abort operation and return to previous values.

NOTE:

The Save starts flashing if Update is clicked, prompting the user to save the modified configuration.

3 Click Update & Save to update and save the configured port status; Midspan configuration is updated accordingly.

5.13.2 All Ports Settings

1 Access the ***Actions on All Ports*** area and select your desired parameters from the drop-down menus.

2 After each selection, click Set to apply the set parameters to all ports; verify that the display is updated accordingly.

3 Click Update to update the configured parameters, or Cancel to abort operation and return to previous values.

NOTE:

The Save starts flashing if Update is clicked, prompting the user to save the modified configuration.

4 Click Update & Save to update and save the configured port status; Midspan configuration is updated accordingly.

6 Troubleshooting

6.1 General

This paragraph provides a symptom and resolution sequence in order to assist in the troubleshooting of operating problems. If the steps given do not solve your problem, do not hesitate to call your local dealer for further assistance. Refer to Table 6-1

Table 6-1: Troubleshooting Steps

Symptom	Corrective Steps
AC LEDs do not illuminate (green)	1. Check your power source 2. Ensure that a proper Ethernet cable is used.
Midspan Ethernet *LINK* LED is off	1. In cases where a Network card (NIC) is connected directly to the Midspan's RJ45 connector, make sure you use a **crossed** Ethernet cable.
Midspan Ethernet *LINK* LED is on and no Ping reply	1. Midspan is shipped with the following default IP 192.168.0.50. Change your Network card IP to 192.168.0.40 and try to Ping again. 2. Connect serial communication RS232 connector from the Midspan to the Host and set Midspan IP to the same IP Network.
Midspan can be 'pinged' from a local Host but when trying to use the Midspan Ping utility, there is no reply.	1. If *Windows Service Pack 2* is utilized, turn off your Firewall application. 2. If Ping is OK, you may consider accessing the advanced Firewall options and enable the Ping option and TFTP, SNMP TRAP ports.

Table 6-1: Troubleshooting Steps

Symptom	Corrective Steps
Midspan is set to DHCP, but no Ping from the Midspan	1. Connect serial communication RS232 connector (using a null modem cable) port to Host COM port. Select ***view*** -> ***Network menu***. In cases where the Midspan was able to get an IP by DHCP, the following display should appear: View Network Parameters (in use) -------------------------------------- Use DHCP : Yes DHCP Server : 172.016.001.001 IP Address : 172.016.004.010 (valid for: 7 Days,21 Hours,6 Min,10 Sec) Subnet Mask : 255.255.000.000 Default Gateway : 172.016.001.254 MAC Address : 00:05:5A:01:67:6F In cases where Midspan wasn't able to get IP by DHCP, the following display appears: View Network Parameters (in use) -------------------------------------- Use DHCP : Yes MAC Address : 00:05:5A:01:67:6F 2. Verify that the Midspan Link LED is ON and that there is a DHCP server on the network.
Software update by TFTP cannot be performed	1. Use the Midspan Ping utility to ping the Host running the TFTP Server application 2. If using Windows, turn off the Firewall application, or enable UDP port 69 3. Verify that appropriate update files package was copied to the TFTP Server root folder.

Table 6-1: Troubleshooting Steps

Symptom	Corrective Steps
Unit cannot be accessed via Telnet	Use Web browser to view *System Configuration->Security WEB page* and make sure that the Telnet checkbox is checked (selected).
When accessing the unit by Telnet, Telnet session is terminated each time the *Configuration* option is pressed.	Log-on to Telnet via the *Configure username & password* option and not via the *Viewer username & password*.
Log-on to unit via Telnet was performed, but after a while the Telnet session is terminated.	Telnet session is terminated in cases where no key was pressed and there was no activity for over more than three (3) minutes.
No SNMP TRAP events are received	1. Use WEB browser to view *System Configuration->Security WEB* page and verify that the *SNMP* checkbox is checked (selected). 2. Check *System Configuration->SNMP WEB page* and verify that the remote SNMP manager IP matches and Trap community string matches the Remote SNMP manager Trap configuration. 3. In cases where Firewall is is being used, enable UDP port 162
SysLog Server IP was set properly, but Log messages are not received	1. In cases where Firewall is being used, enable UDP port 514
One of the ports was disabled. After the unit was turned Off and On, it suddenly turned On again.	1. When changing port status, verify that the Save & Update button is pressed. 2. Verify that the PD is compatible to the detection method of the system.

Table 6-1: Troubleshooting Steps

Symptom	Corrective Steps
When using a web Browser and accessing View Status Web page, all ports are red illuminated and a question mark appears	If the Midspan doesn't provide power to PoE PDs, try to update the internal firmware. If problem persists, contact technical support.

7 Software Update

7.1 Architecture

There are two types of software associated with the Power over Ethernet (PoE) Midspan:

- Midspan Application – Update of Midspan management application (including all Web pages) that provide remote NMS management capabilities
- Midspan Firmware – Update firmware used to manage PoE Power ports.

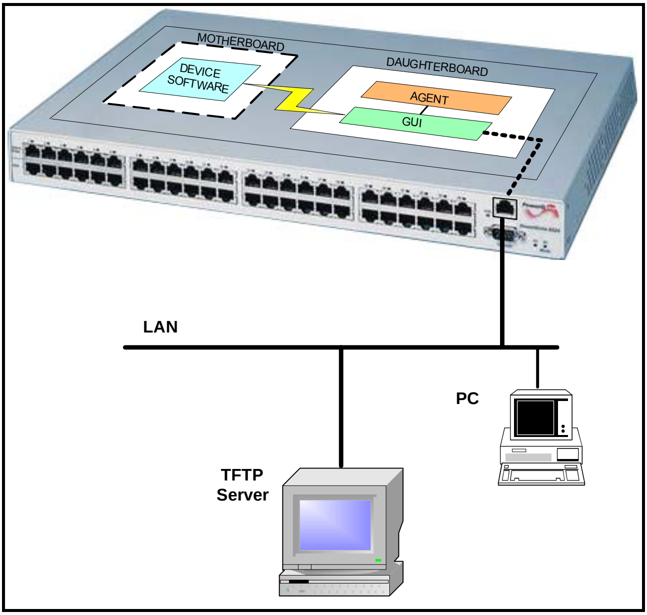
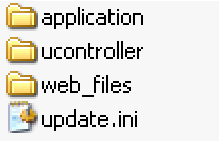


Figure 7-1: System Software Architecture

7.2 Software Upgrade

7.2.1 General

Software update is required when a newer software version is issued by the vendor, or when malfunction occurs and the current version must be re-installed. To perform software update, the user must verify that it has TFTP Server application and that an update software files package is available (see image bellow)



application
ucontroller
web_files
update.ini

Software update menu can be accessed only by Telnet (remote software update) or Console (local software update).

- ***Telnet*** *(using RJ-45)* – Provides remote update capabilities, with no need to be in the site itself.
- ***Console*** *(RS232 connector)* – Provides local access to software update menus.

NOTE:

In both cases software update is performed by TFTP. The Telent or Console options are utilized in order to access the appropriate menu and activate software update via TFTP.

NOTE:

When accessing the system via Telnet, the user is prompted to type user name and password. If upgrading is performed locally, user name and password are not required.

7.2.2 Upgrade Process

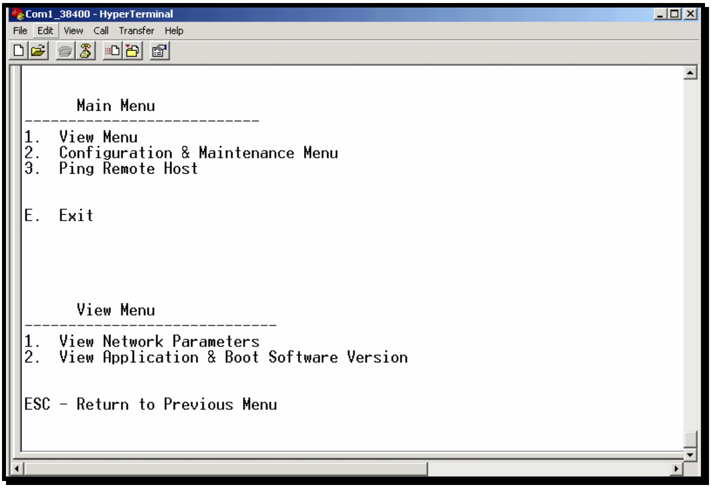
➢ To Upgrade the software:

1 Install the TFTP software as described in Para. 3.5: "TFTP Server Configuration".

2 Copy the software update files to your TFTP Server desired folder. It is recommended that the TFTP Server will be used on the same Ethernet network as the Midspan.

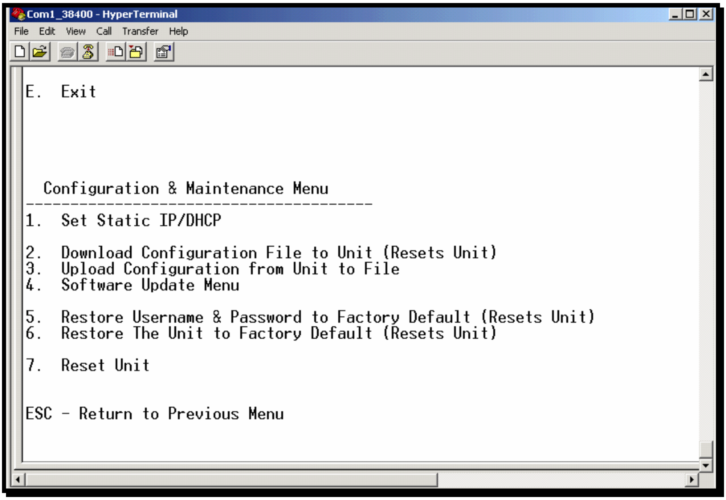
3 Activate the HyperTerminal application; HyperTerminal main screen appears (empty).

4 Click ENTER or ESC; the main menu appears;



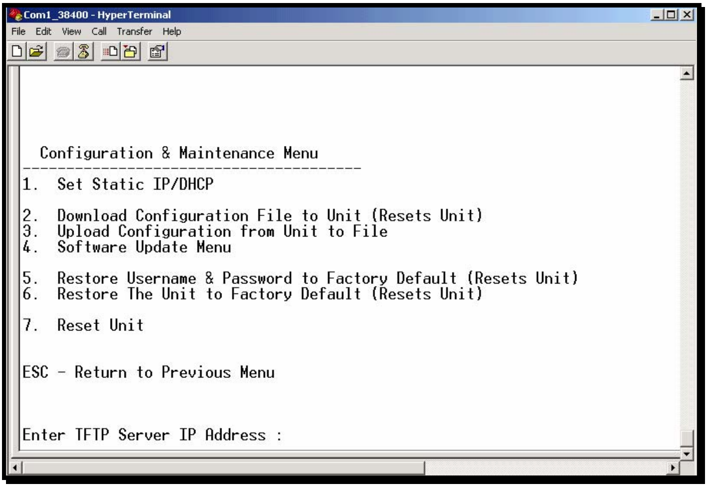
```
       Main Menu
---------------------------
1.   View Menu
2.   Configuration & Maintenance Menu
3.   Ping Remote Host


E.   Exit




       View Menu
-----------------------------
1.   View Network Parameters
2.   View Application & Boot Software Version


ESC - Return to Previous Menu
```

5 Select the *Configuration & Maintenance Menu* (2); the following screen appears:



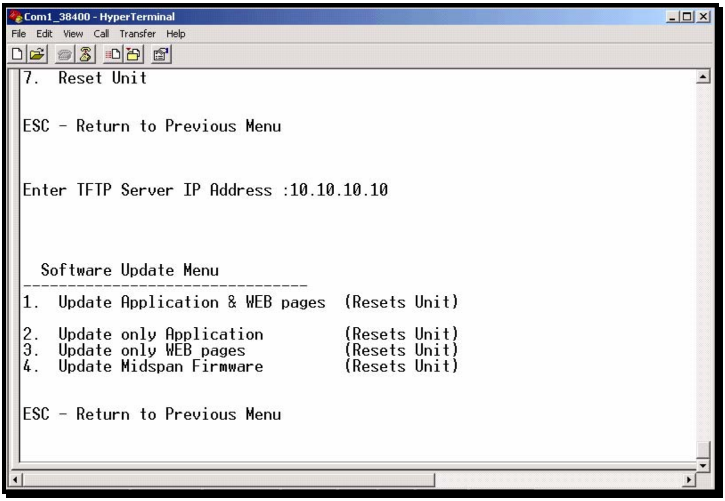
```
E.   Exit



  Configuration & Maintenance Menu
---------------------------------------
1.   Set Static IP/DHCP

2.   Download Configuration File to Unit (Resets Unit)
3.   Upload Configuration from Unit to File
4.   Software Update Menu

5.   Restore Username & Password to Factory Default (Resets Unit)
6.   Restore The Unit to Factory Default (Resets Unit)

7.   Reset Unit


ESC - Return to Previous Menu
```

6 Select the *Software Update Menu* (4); the following screen appears:



```
  Configuration & Maintenance Menu
---------------------------------------
1.   Set Static IP/DHCP

2.   Download Configuration File to Unit (Resets Unit)
3.   Upload Configuration from Unit to File
4.   Software Update Menu

5.   Restore Username & Password to Factory Default (Resets Unit)
6.   Restore The Unit to Factory Default (Resets Unit)

7.   Reset Unit


ESC - Return to Previous Menu


Enter TFTP Server IP Address :
```

7 Type the appropriate TFTP server's IP address; the following screen appears:



```
7.  Reset Unit

ESC - Return to Previous Menu


Enter TFTP Server IP Address :10.10.10.10



  Software Update Menu
--------------------------------
1.  Update Application & WEB pages  (Resets Unit)

2.  Update only Application         (Resets Unit)
3.  Update only WEB pages           (Resets Unit)
4.  Update Midspan Firmware         (Resets Unit)

ESC - Return to Previous Menu
```

8 Select the application update option and then click *ENTER*.

An update.ini TFTP file containing a list of all files is downloaded to the Midspan.

Upon completion of files update, the Midspan resets itself (in cases where Telnet connection is being used, Telnet connection is disconnected).

Revision History

Revision Level / Date	Para. Affected/page	Description
1.0 / January 05		First Release
1.1 / September 05		S/W RELEASE 2